# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-123496
(43)Date of publication of application : 26.04.2002

(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 9/08
H04N 5/44
H04N 7/16
H04N 7/167

(21)Application number : 2000-316395 (71)Applicant : SONY CORP
(22)Date of filing : 17.10.2000 (72)Inventor : EZAKI TADASHI

(54) DEVICE AND METHOD FOR RECEIVING CONTENTSSTORAGE MEDIUM AND SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents receiver corresponding to a plurality of RMPs(Right Management and; Protection) systems drawn up in each contents distribution system.
SOLUTION: Only formats for regulating the specifications of the RMPs composed of information such as contents chargingsecurity and copyright protection are unified. Each contents provider inputs enciphered contents and right processing information in a format conforming to the unified specification. A contents user side can decode and utilize contentsregardless of their PMP systemson the same contents receiver only by preparing a plurality of functions corresponding to the respective RMP systems.

CLAIMS

[Claim(s)]
[Claim 1]It is content reception equipment which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) systemA content reception means to receive contents distributingand an identification device which identifies right management and a

protection system of receiving contentsContent reception equipment providing a right processing means which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said identification device.

[Claim 2]Right management and a protection system A cipher system of contentsdistribution systems of a keya contents decryption systemA transmission system of accounting information or keysarchive-medium control informationa system of mutual recognitionAPS (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)The content reception equipment according to claim 1 specifying an indispensable item to content purchase and contents use of viewing limit information etc.

[Claim 3]The content reception equipment according to claim 1 characterized by what it has two or more kinds of right management and protection modulessaid right processing means chooses corresponding right management and protection module based on a discriminated result by said identification deviceand right processing of receiving contents is performed for.

[Claim 4]Have right management and a protection module acquisition means which acquires right management and a protection module from the exteriorand said right processing meansThe content reception equipment according to claim 1 characterized by what right processing of receiving contents is performed for using right management and a protection module acquired from the exterior via said right management and protection module acquisition means based on a discriminated result by said identification device.

[Claim 5]Have right management and a protection module generation means to generate right management and a protection module automatically according to specification description of right management and a protection systemand said right processing meansThe content reception equipment according to claim 1 characterized by what right processing of receiving contents is performed for using right management and a protection module generated by said right management and protection module generation means.

[Claim 6]The content reception equipment according to claim 1 including a contents storage means which accumulates contents.

[Claim 7]The content reception equipment according to claim 1 characterized by what contents before right processing by said right processing means are stored in said contents storage means for including a contents storage means which accumulates contents.

[Claim 8]The content reception equipment according to claim 1 characterized by what contents after right processing by said right processing means are stored in said contents storage means for including a contents storage means which accumulates contents.

[Claim 9]Said content reception meansincluding further a contents storage means

which receives contents distributed in form enciphered with a predetermined keyand accumulates contents said right processing meansThe content reception equipment according to claim 1 characterized by what enciphered content which received is decryptedand is stored in a contents storage means after re-enciphering with other keys.

[Claim 10]Contents distributed in form that said content reception means was enciphered with a predetermined keyAndincluding further a contents storage means which receives an enciphering key which enciphered this key and accumulates contents said right processing meansThe content reception equipment according to claim 1 characterized by what a received enciphering key is decryptedand is stored in a contents storage means with enciphered content after re-enciphering with other keys.

[Claim 11]The content reception equipment according to claim 1wherein said right processing means accumulates a log of right processing of receiving contents.

[Claim 12]The content reception equipment according to claim 1 characterized by what said right processing means carries out APS (Analog Protection System) processingand does for the external output of the regenerative signal of contents after right processing according to specification description of applicable right management and protection system.

[Claim 13]The content reception equipment according to claim 1wherein said right processing means enciphers and carries out the external output of the contents after right processing.

[Claim 14]It is a contents receiving method which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) systemA content reception step which receives contents distributingand a discernment step which identifies right management and a protection system of receiving contentsA contents receiving method providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[Claim 15]Right management and a protection system A cipher system of contentsdistribution systems of a keya contents decryption systemA transmission system of accounting information or keysarchive-medium control informationa system of mutual recognitionAPS (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)The contents receiving method according to claim 14 specifying an indispensable item to content purchase and contents use of viewing limit information etc.

[Claim 16]The contents receiving method according to claim 14 characterized by what it has two or more kinds of right management and protection modulescorresponding right management and protection module are chosen in said right processing step based on a discriminated result by said discernment stepand right processing of

receiving contents is performed for.
[Claim 17]Based on a discriminated result by said discernment stepit has further right management and a protection module acquisition step which acquires applicable right management and protection module from the exteriorThe contents receiving method according to claim 14 characterized by what right processing of receiving contents is performed for in said right processing step using right management and a protection module acquired from the exterior by said right management and protection module acquisition step.
[Claim 18]Have further right management and a protection module generation step which generates right management and a protection module automatically according to specification description of right management and a protection systemand in said right processing step. The contents receiving method according to claim 14 characterized by what right processing of receiving contents is performed for using right management and a protection module generated by said right management and protection module generation step.
[Claim 19]The contents receiving method according to claim 14 containing a contents storage step which accumulates contents which received.
[Claim 20]The contents receiving method according to claim 14 containing a contents storage step which stores contents before right processing by said right processing step.
[Claim 21]The contents receiving method according to claim 14 containing a contents storage step which stores contents after right processing by said right processing step.
[Claim 22]Contents distributed in form enciphered with a predetermined key at said content reception step are receivedThe contents receiving method according to claim 14 characterized by what it has for a contents storage step stored after re-enciphering receiving contents decrypted in said right processing step with other keys.
[Claim 23]Contents distributed in said content reception step in form enciphered with a predetermined keyAnd the contents receiving method according to claim 14 characterized by what an enciphering key which enciphered this key is received and it has for a contents storage step stored with enciphered content after re-enciphering a key decrypted in said right processing step with other keys.
[Claim 24]The contents receiving method according to claim 14 provided with a log accumulation step which accumulates a log of right processing of receiving contents in said right processing step.
[Claim 25]A regenerative signal of contents after right processing by said right processing stepThe contents receiving method according to claim 14 characterized by what APS (Analog Protection System) processing is carried out according to specification description of applicable right management and protection systemand it has an external output step which carries out an external output for.
[Claim 26]The contents receiving method according to claim 14 characterized by what

it has for an external output step which enciphers and carries out the external output of the contents after right processing by said right processing step.
[Claim 27]. Are characterized by comprising the following. So that reception of contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) system may be performed on computer systems. A storage which stored described computer software physically in computer-readable form.
A content reception step to which said computer software receives contents distributing.
A discernment step which identifies right management and a protection system of receiving contentsand a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[Claim 28]A server comprising:
A means to accumulate two or more right management and protection modules corresponding to each right management and protection system.
A means to answer a demand having contained identification information of right management and a protection systemand to transmit applicable right management and protection module.

[Claim 29]A server comprising:
A means to accumulate two or more right management and protection modules corresponding to each right management and protection system.
A means to answer an inquiry based on identification information and to change contents using applicable right management and protection module.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the content reception equipment and the contents receiving method which receive the contents distributed via a broadcast wavea networketc.It is related with the content reception equipment and the contents receiving method with which a specific user receives the pay content distributed in the form that a moviemusicetc. were enciphered especially.
[0002]As for this inventioncontents work and providing agentssuch as a movie and musicstart the content reception equipment and the contents receiving method to receive in detail for the enciphered content distributed via brokerssuch as a

broadcasting organization and an Internet Service Providerand it especiallyIt is related with the content reception equipment and the contents receiving method with which contents work and the providing agent itself receive the contents which distribute fee collectionsecurityetc. about contents use with a controllable form.
[0003]
[Description of the Prior Art]It is increasingly dealt with on information machines and equipmentsuch as a computerwith innovation of the information technology of these days as contents by which various mediasuch as an image and musicwere digitized. These contents can be distributed by development of information and communication technology using broadcast of a satellitea terrestrial waveetc.or a broad-based network like the Internet.
[0004]Distribution of an image content or a music content is already carried out partly. According to contents distribution technologya conventional commercial distribution course and physical medium are omissible. Even if it is the consumers of a remote placedesired image and music title can be obtained easily. Contents work volition leads also to development of increase and the whole industry by making higher profits with the position by the side of contents work and a providing agent by quick and efficient contents selling. [0005]For examplein the server type and accumulation type broadcasting system on condition of the TV receiver containing the mass hard disk driveProfits are certainly securable by enciphering and distributing contentssuch as a moviein the contents distribution contractor of a broadcasting station or othersand charging the key for decryption to a contents purchaseri.e.a televiewerat the time of distribution.
[0006]Such a content reception form is also called a CAS (Conditional Access System (limited reception)) system. In drawing 14the general-view composition of the contents distribution system of a CAS base is illustrated.
[0007]The content provider who makes or provides contents for distributionsuch as an image and musicin the contents distribution system shown in the figureIt comprisesa contents distribution entrepreneur who distributes to consumers the contents which a content provider provides via a broadcast wave or a networkand the consumersi.e.three persons of a general userwho receive contents.
[0008]The broadcasting organization for whom the contents distribution entrepreneur used broadcasting satellitessuch as BS(Broadcasting Satellite: broadcasting satellite) CS (Communication Satellite: communications satellite)for exampleIt comprises an Internet Service Provider etc. which manage the broadcasting organization using a terrestrial wave or the connection service to the Internetand the variety-of-information contents providing service on the Internet.
[0009]The general user is installing the content reception machine which receives contents distributingfor example in a house. A TV receiver like STB (Set Top Box) may be sufficient as the content reception machine which receives the contents through a broadcast wavefor example. A common computer system like a personal

computer (PC) may be sufficient as the content reception machine which receives contents via the Internetfor example. A content reception machine contains a hard disk driveand it is preferred that it is a receiver corresponding to the accumulated type broadcast which can accumulate a long timei.e.an imageand a lot of music contents.

[0010]In order for a content reception machine to receive contents via a broadcast waveit is necessary to equip the CAS (limited reception) card corresponding for every broadcasting organization. In order to receive contents via the Internetwhile acquiring a user account (user qualification) from a predetermined Internet Service Provider beforehandit is necessary to carry out an Internet connectivity via a nearby access point at the time of content purchase.

[0011]What is necessary is just to use the time of CAS card (or receiver which contained CAS) purchasefor examplein order for a broadcasting organization to collect the expenses and profits which contents distribution takes. What is necessary is just to add the contents fee amount equivalent to the fee paid every monthfor examplein order for an Internet Service Provider to collect the expenses and profits which contents distribution takes. Howeverthe charging system by the CAS system or a user account aims to let a contents distribution entrepreneur control the fee collection to each consumersi.e.contents user.

There is nothing under a content provider's control.

In other wordseven if a content provider uses CAS of the contents distribution entrepreneur bodyetc.he cannot secure his profits.

[0012]In order for a content provider to collect a contents fee from general consumersIt is mentioned that the content provider itself decides upon contents provision systems (referred to as RMP (Right Management & Protection) below)such as a contents feesecurityand copyright protection. In RMPmore specifically The system of encryptionthe distribution systems of a keya contents decryption systemThe transmission system of accounting information or keysarchive-medium control informationthe system of mutual recognitionThe indispensable item is included in the content purchase and contents use of APSs (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)viewing limit informationetc. In the user and consumer side of contentsby preparing the content reception machine which mounted the RMP module corresponding to a content providerthe contents distributing which uses a content provider as a supply source can be purchased on the success reverse sideand it can usenamelyview and listen to it. It may be made to leave the batch management of accounting information to the settlement-of-accounts organization besides a content provider like a control center.

[0013]Howeverthe actual condition is deciding upon the RMP system about a contents feesecurityand copyright protection variously generally for every contents distribution system which each content provider provides. if a contents distribution system is different even if it is the same music content distribution and movie

contents distribution under the environment where two or more systems are intermingled -- the same contents receiver top -- if -- that is [ it cannot decrypt ]it falls into the situation where contents cannot be used.
[0014]For exampleif a contents user is going to purchase contentstwo or more content providersi.e.distribution systemThe hardware or software of a content reception machine must be prepared for every distribution systemit is inconvenient to a user or excessive expenses are needed. As a conclusion with the troublesome content purchase methodwhen a user's contents refrainment from buying arisesthe profits of contents offer / distribution enterprise will make little increaseand the whole enterprise may become calm.
[0015]
[Problem to be solved by the invention]The purpose of this invention is to provide the outstanding content reception equipment and contents receiving method with which a specific user can receive suitably the pay content distributed in the form that a moviemusicetc. were enciphered.
[0016]. The further purpose of this invention can receive suitably the enciphered content which contents work and providing agentssuch as a movie and musicdistribute via brokerssuch as a broadcasting organization and an Internet Service Provider. It is in providing outstanding content reception equipment and contents receiving method.
[0017]The further purpose of this invention is for contents work and the providing agent itself to provide the outstanding content reception equipment and contents receiving method which can receive suitably the contents which distribute fee collectionsecurityetc. about contents use with a controllable form.
[0018]The further purpose of this invention is to provide outstanding content reception equipment and a contents receiving method which can respond to two or more RMP (Right Management & Protection) systems upon which it is decided for every contents distribution system.
[0019]
[Means for Solving the Problem and its Function]This invention is made in consideration of an aforementioned problemand the 1st sideIt is content reception equipment which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) systemA content reception means to receive contents distributingand an identification device which identifies right management and a protection system of receiving contentsIt is content reception equipment providing a right processing means which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said identification device.
[0020]Work / offer entrepreneur of contents distributes contents in form that encryption etc. were protected according to right management and a protection system called RMP. Generallyvarious right management and protection system are

adopted for every contents work / offer entrepreneur.
[0021]Only by unifying only a form which specifies specification of right management and a protection system according to content reception equipment concerning the 1st side of this inventionAn identification device can identify right management and a protection system of receiving contentsand the right processing means can carry out right processing of the receiving contentsusing selectively right management and a protection system applicable based on this discriminated result.
[0022]Thereforeonly by preparing beforehand a function corresponding to each right management and protection systemeven if it is a case where contents in accordance with which right management and protection system are receivedit can respond to several different contents distribution systems using one set of a content reception machine. It becomes unnecessary that isto be able to decrypt contents on the same contents receiverto be able to appropriate for the useand to prepare apparatussuch as a receiver for every distribution system.
[0023]Among each contents work and offer / distribution entrepreneurargument involving standardization of contents distribution systemssuch as RMP specification descriptioncan be calmed down. Compatibility and flexibility of contents distributing between each contents work and offer / distribution entrepreneur can be raised. Convenience increases in a contents user.
[0024]Here right management and a protection system to say A cipher system of contentsdistribution systems of a keyA contents decryption systema transmission system of accounting information or keysarchive-medium control informationA system of mutual recognitionAPS (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)An indispensable item is specified to content purchase and contents use of viewing limit information etc.
[0025]Content reception equipment may be beforehand provided with two or more kinds of right management and protection modules. In such a casesaid right processing means can choose corresponding right management and protection module based on a discriminated result by said identification deviceand can perform right processing of receiving contents.
[0026]Or content reception equipment may be provided with right management and a protection module acquisition means which acquires right management and a protection module from the exterior. In such a casesaid right processing means can perform right processing of receiving contents using right management and a protection module acquired from the exterior via said right management and protection module acquisition means based on a discriminated result by said identification device.
[0027]Or content reception equipment may be provided with right management and a protection module generation means to generate right management and a protection module automatically according to specification description of right management and a protection system. In such a casesaid right processing means can be done

[ performing right processing of receiving contents using right management and a protection module generated by said right management and protection module generation meansor ].
[0028]Content reception equipment may include a contents storage means which accumulates contents. For examplecontents before right processing by said right processing means and after right processing are storable in said contents storage means.
[0029]Contents which said content reception means receives are enciphered with a predetermined keyfor example. In such a casesaid right processing means decrypts enciphered content which receivedand after re-enciphering with other keysit may be made to store it in a contents storage means. By such compositioncontents after right processing can be protected further.
[0030]Contents which said content reception means receives also receive an enciphering key which enciphered this key further while being distributed in form enciphered with a predetermined keyfor example. In such a casesaid right processing means decrypts a received enciphering keyand after re-enciphering with other keysit may be made to store it in a contents storage means with enciphered content. By such compositioncontents after right processing can be protected further.
[0031]It may be made for said right processing means to accumulate a log of right processing of receiving contents. In such a casea settlement-of-accounts organization can perform exact accounting byfor exampletransmitting an accumulated log to a predetermined settlement-of-accounts organization periodically or irregularly.
[0032]Said right processing means carries out APS (Analog Protection System) processing according to specification description of applicable right management and protection systemand may be made to carry out the external output of the regenerative signal of contents after right processing. In such a casea video recovery signal after right processingetc. can be protected.
[0033]Said right processing means enciphers contents after right processingand may be made to carry out an external output. In such a casea case where contents are transmitted to other information machines and equipmentfor example by a home network course like IEEE 1394Contents can be protected even if it is a case where transmit contents to a computer system like a personal computer (PC) via LANand it processes using application.
[0034]The 2nd side of this invention is a contents receiving method which receives contents distributed in conformity with prescribed right management and protection (Right Management &Protection:RMP) systemA content reception step which receives contents distributingand a discernment step which identifies right management and a protection system of receiving contentsIt is a contents receiving method providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[0035]Only by unifying only a form which specifies specification of right management and a protection system according to the contents receiving method concerning the 2nd side of this inventionA discernment step can identify right management and a protection system of receiving contentsand can carry out right processing of the receiving contents in a right processing stepusing selectively right management and a protection system applicable based on this discriminated result.
[0036]In said right processing stepbased on a discriminated result by said discernment stepcorresponding right management and protection module are chosenand it may be made to perform right processing of receiving contents.
[0037]Or based on a discriminated result by said discernment stepit may have further right management and a protection module acquisition step which acquires applicable right management and protection module from the exterior. In such a casein said right processing stepright processing of receiving contents can be performed using right management and a protection module acquired from the exterior by said right management and protection module acquisition step.
[0038]Or it may have further right management and a protection module generation step which generates right management and a protection module automatically according to specification description of right management and a protection system. In such a casein said right processing stepright processing of receiving contents can be performed using right management and a protection module generated by said right management and protection module generation step.
[0039]A contents storage step which accumulates contents which received may be included. For exampleit may be made to store contents before right processing by said right processing stepand after right processing.
[0040]At said content reception stepwhen receiving contents distributed in form enciphered with a predetermined keyit may have a contents storage step stored after re-enciphering receiving contents decrypted in said right processing step with other keys.
[0041]Contents distributed in said content reception step in form enciphered with a predetermined keyAnd after re-enciphering a key decrypted in said right processing step with other keysit may be made to have a contents storage step stored with enciphered contentwhen receiving an enciphering key which enciphered this key.
[0042]It may have a log accumulation step which accumulates a log of right processing of receiving contents in said right processing step. In such a casea settlement-of-accounts organization can perform exact accounting byfor exampletransmitting an accumulated log to a predetermined settlement-of-accounts organization periodically or irregularly.
[0043]It may have an external output step which carries out APS (Analog Protection System) processingand carries out the external output of the regenerative signal of contents after right processing by said right processing step according to specification description of applicable right management and protection system.

[0044]It may have an external output step which enciphers and carries out the external output of the contents after right processing by said right processing step.
[0045]The 3rd side of this inventionSo that reception of contents distributed in conformity with prescribed right management and protection (Right Management &Protection:RMP) system may be performed on computer systems. In computer-readable formare described computer software the storage stored physicallyand said computer softwareA content reception step which receives contents distributingand a discernment step which identifies right management and a protection system of receiving contentsIt is a storage providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.
[0046]A storage concerning the 3rd side of this invention is a medium which provides computer software physically in a computer-readable form to computer systems of flexibility which can execute various program codesfor example. Attachment and detachment of CD (Compact Disc)FD (Floppy Disc)MO (Magneto-Optical disc)etc.etc. are free for such a mediumand it is a storage of portabilityfor example. Or it is also technically possible to provide specific computer systems with computer software in computer-readable form via transmission mediasuch as a network (a network does not ask distinction of radio and a cable)etc.
[0047]Such a storage defines a collaboration relation on structure of computer software and a storage for realizing a function of predetermined computer softwareor a function on computer systems. By installing predetermined computer software in computer systems via a storage concerning the 3rd side of this inventionif it puts in another wayOn computer systemsa collaboration operation is demonstrated and the same operation effect as content reception equipment and a contents receiving method concerning each 1st [ of this invention ] and 2nd sides can be obtained.
[0048]A means by which the 4th side of this invention accumulates two or more right management and protection modules corresponding to each right management and protection systemIt is a server provided with a means to answer a demand having contained identification information of right management and a protection systemand to transmit applicable right management and protection module.
[0049]A means by which the 5th side of this invention accumulates two or more right management and protection modules corresponding to each right management and protection systemIt is a server possessing a means to answer an inquiry based on identification information and to change contents using applicable right management and protection module.
[0050]The purposethe featureand an advantage of further others of this invention will become clear [ rather than ] by detailed explanation based on an embodiment and Drawings to attach of this invention mentioned later.
[0051]
[Mode for carrying out the invention]An embodiment of this invention described below

explains content reception equipment which can respond to two or more RMP(s) upon which it is decided for every contents distribution system.
[0052]RMP is the abbreviation for Right Management & Protectionand is a concept used by TV Anytime Forum. becoming a problem in a contents distribution enterprise through broadcast or a network -- an illegal use of contents -- merely seeing and merely hearing it -- it is . If this kind of malfeasance overrunscontents work and offer / distribution entrepreneur's just profits will not be guaranteedbut it will be concerned also with enterprise fate. In other wordsuse right management of contents and protection are requiredand RMP bears this.
[0053]In RMPmore specifically A system of encryptiondistribution systems of a keya contents decryption systemA transmission system of accounting information or keysarchive-medium control informationa system of mutual recognitionAn indispensable item is included in content purchase and contents use of APSs (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)viewing limit informationetc.
[0054]Only a form which specifies specification of RMP which consists of these items is unifiedand each contents offer entrepreneur should just input enciphered content and right processing information into contents in form in accordance with this specification. In such a casein the sideconsumersi.e.a contents userwho receive and use contents. Even if it is the contents based on what kind of RMP system by preparing two or more functions corresponding to each RMP systemit can decrypt on the same contents receiver and can appropriate for the use.
[0055]RMP specification description can be described as a part of metadata which accompanies contents distributingfor example. Belowa portion relevant to RMP specification description will be called "right processing metadata" among metadata. For examplein the case of digital broadcasting etc.metadata can be distributed as data for data broadcasting which accompanies a volume on program book.
[0056]Conceptual composition of a RMP module is shown in drawing 1. A RMP module is built in and used for a content reception machine of a form of STB (Set Top Box) or othersand can be mounted using a module of predetermined hardware or softwarefor example. As shown in the figurea RMP module has composition provided with some interfaces for outputting and inputting data about receiving contents.
[0057]The contents downloaded via networkssuch as contents received via broadcast of a satellite wave or a terrestrial wave or the Internetare stored in mass storage devicessuch as a hard disk drivewith metadata. A RMP module inputs receiving contents in the state before right processing directlywithout passing a hard disk drive course or a hard disk drive.
[0058]Encryption is given to contents bodiessuch as an image and musicfor the purpose of contents protection. Thereforethe decipherment function (Decryptor) for solving enciphered content is requiredand a RMP module has an interface for an enciphered content input which inputs enciphered content by the specified

cryptographic algorithm.
[0059]Although metadata is distributed corresponding to each contentsin itthe information which shows the right processing and the required right protection about contentsi.e.right processing metadatais included.
[0060]The copy control information etc. of the keys for solving contentsthe terms of purchase of contentsa service conditionand the decoded contents are included in right processing metadata. A RMP module has an input interface of right processing metadata which inputs the information about right processing or protection according to a regular format.
[0061]Contents distributing is encipheredfor example by a contents keyand this contents key is transmitted with enciphered content with a form further enciphered with a distribution key (Distribution Key). In a RMP modulea distribution key is helda contents key enciphered using this distribution key can be decodedand enciphered content can be further decoded using a decoded contents key. While being able to perform contents distribution safely according to such encryption and a transmission systemchanging a contents key for every contentsby a RMP moduleenciphered content can be decoded by holding a single distribution keyand it can appropriate for the use. It may be made for a right processing metadata input interface of a RMP module to input an enciphered content key as right processing metadata.
[0062]Specification about fee collection for contents use upon which it decides in contents work / offer entrepreneur is also included in right processing metadataand it may be made for a right processing metadata input interface of a RMP module to input this.
[0063]As specification about fee collectionprice informationservice conditions (reproduction fee collection in every timenumber-of-times restrictions which specified the refreshable number of times beforehandtime limitation made refreshable till the predetermined dateetc.)etc. can be specifiedfor example.
[0064]For the accounting to a contents usersettlement-of-accounts organizations other than a contents work and offer / distribution entrepreneur like a control center may be established. It connects with such a control center and a RMP module has an accounting interface for performing the transaction about fee collection or settlement of accounts. Whenever itfor examplereproduces the contents accumulated on the hard disk drivea fee collection log is generatedand it connects with a control center for every prescribed periodand a RMP module transmits a log. On the other handthe control center can perform fee collection and settling processing based on the log sent by each contents user.
[0065]It is as having already stated to have the interface for enciphered content for a RMP module to input the receiving contents before right processing. A RMP module for the interface for accumulating the contents after right processing in a hard disk drive again for the use covering several times of contentsand permanent / semipermanent preservation of contentsIt has the interface for storing the contents

after right processing on removable mediassuch as DVD (Digital Versatile Disc). The interface for the contents storage and reproduction after such right processing can specify existencean authentication methodetc. of the control to mediasuch as encryption of the contents for accumulationand a decoding at the time of reproductionand the attestation to media.
[0066]A RMP module is provided with an external output interface for reproducing receiving contents or contents read from a hard disk drive or a removable media with a display or other external instruments. In an example shown in drawing 1it has an analog output interface for carrying out a display output on a display as a video signaland a digital output interface for transmitting contents to an external instrument via home networkssuch as IEEE 1394. An analog output interface adopts APS (Analog Protection System) etc. for contents protection of analog format. A macro visionCGMS(Copy Generation Management System)-ASCMS which embed copy control information at a predetermined scanning line of a vertical blanking intervaletc. are contained in APS. Attestation bus encryption like 1394CP besides transmitting contents encryptionetc. are controllable by a digital output interface.
[0067]Contents after right processing can be transmitted and processing using desired application can be performed on an information management system like a personal computer (PC). A RMP module is provided with the host / interface for applications for outputting contents to an external information management system in an example shown in drawing 1. A host / interface for applications controls encryption of transmitting contentsetc.
[0068]Mounting with hardware components for exclusive use can also realize a RMP module also by executing a predetermined program code on a general-purpose processor. Along with contents distributingdistribution and distribution of specification about RMP can be done as right processing metadata (above-mentioned).
[0069]An example of a RMP specification description format is shown below.
[0070]
[Mathematical formula 1]

[0071]In the RMP specification description format shown above.The identification information (RMP ID) for identifying the system of RMP is included in the beginningand also. The encryption algorithm which enciphers contents distributingthe encryption algorithm which enciphers the contents key Ks used for encryption of contents distributingThe format for accumulating the authentication algorithm and log which are used for the storage key Kst used when accumulating the encryption algorithm and contents distributing which encipher the distribution key Kd used at the time of contents distributionand mutual recognitionetc. can be specified. Generally as a cipher systemDES (Data Encription Standard)Multi2etc. are used.
[0072]It is decided upon the specification description as RMP for every contents work

/ offer entrepreneur. Since RMP was conventionally fixed and used for every contents distribution systemin order to receive offers of contents from two or more systemsexcessive expensessuch as preparing a new content reception machinewere required. On the other handby specifying the interface for inputting into the specification description of RMPand RMP by this inventionIt can respond to security systemssuch as a contents fee in two or more contents distribution systemsand encryptionand a copyright protection system on the same contents receiver by the RMP module which decoded the specification or suited the specification coming to hand.

[0073]As one real original form voice of this inventionby a content reception machine or the contents recording reproduction inside of a plane. Two or more hardware RMP modules which mounted different RMP specification are preparedand changing and using for a hardware RMP module which suits for every receiving contents is mentioned.

[0074]A RMP module is constituted as a software module as other real original form voiceDownloading a software module which suits for every receiving contents from a predetermined serveror analyzing right processing metadata and generating a desired software module automatically by a content reception machine side are mentioned.

[0075]Two or more hardware RMP modules which mounted different RMP specification are prepared for drawing 2and composition of the content reception machine 10 of form changed and used for a hardware RMP module which suits for every receiving contents is illustrated typically.

[0076]The content reception machine 10 shown in the figure The front end section 11 and the CAS treating part 12It comprises the hard disk drive 13A for contents storage and 13Bthe RMP identification part 14and the two RMP modules (plurality) 1 and the RMP module 2 based on RMP specification description differentrespectively.

[0077]The front end section 11 performs tuning of the broadcast wave of a predetermined channeli.e.channel selection processingand recovery processing of received data.

[0078]The CAS treating part 12 cancels the scramble processing applied to broadcast contents based on the contract about CAS (Conditional Access System (limited reception)) exchanged among contents distribution entrepreneurs (descrambling). In the digital broadcasting in JapanBS and CS adopt the scrambling system called common "MULTI2." Howeversince the CAS processing itself does not relate to the summary of this inventionit is not explained any more here.

[0079]The hard disk drives 13A and 13B are used for accumulation of receiving contents. One hard disk drive 13A is used for accumulation of the contents of the state before the right processing by a RMP moduleandmore specificallythe hard disk drive 13B of another side is used for accumulation of the contents of the state after right processing. Howeverthe hard disk drives 13A and 13B may be the separate storage areas (partition) which do not need to be isolated systems mutuallyfor

examplewere physically assigned on the single hard disk.
[0080]In this examplethe peculiar identification information (RMP ID) for identifying the system is assigned to RMP described as a part of right processing metadata. The RMP identification part 14 enables operation of the direction corresponding to RMP ID which read right processing metadata from the hard disk drive 13Aidentified RMP IDand was identified among the two RMP modules (plurality) 1 and the RMP module 2.
[0081]The RMP module 1 and the RMP module 2 are provided with some interfaces (above-mentioned) for processing the right processing metadata which accompanies contentssuch as an enciphered movie and musicand contents. The RMP module 1 or the RMP module 2 energized by the RMP identification part 14It operates as the RMP specification description described as right processing metadataand contents processing of a decoding of enciphered contentthe external output as reproduction contentsthe hard disk drive 13Bstoring in a removable mediaetc.etc. is performed.
[0082]To drawing 3the composition of the content reception machine 20 concerning other embodiments is illustrated typically. The content reception machine 20 prepares two or more hardware RMP modules which mounted different RMP specificationis changed to the hardware RMP module which suits for every receiving contentsand is used.
[0083]In an example shown in the figurethe content reception machine 20 has the front end section 21the hard disk drive 23the RMP identification part 24each RMP module 1 and the RMP module 2and composition by which interconnection was carried out via the data bus 26 with the same decoder output equipment 25.
[0084]The front end section 21 performs tuning of a broadcast wave of a predetermined channeli.e.channel selection processingand recovery processing of received data. Howeveralthough not illustratedwhen receiving contents from a predetermined service provider via wide area networkssuch as the Internetto instead of [ which does not pass a broadcast wave ]a Network Interface Card can realize the front end section 21.
[0085]The hard disk drive 23 is used in order to accumulate contents of a state before right processing by a RMP module or to accumulate contents of a state after right processing.
[0086]The peculiar identification information RMP ID for identifying the system is assigned to RMP described as right processing metadata. The RMP identification part 24 enables operation of a thing corresponding to RMP ID which read right processing metadata from the hard disk drive 23identified RMP IDand was identified among the two RMP modules (plurality) 1 and the RMP module 2.
[0087]The RMP module 1 and the RMP module 2 are provided with some interfaces (above-mentioned) for processing right processing metadata which accompanies contentssuch as an enciphered movie and musicand contents. The RMP module 1 or the RMP module 2 energized by the RMP identification part 24It operates as RMP specification description described as right processing metadataand contents

processing of a decoding of enciphered contentan external output as reproduction contentsthe hard disk drive 23storing in a removable mediaetc.etc. is performed. When receiving contents from a contents distribution entrepreneur who adopts a CAS systemit may be made to carry a CAS module which performs corresponding decryption and descrambling processing on a RMP module.

[0088]The decoder output equipment 25 performs decoding and an external output of reproduction contents after right processing. For exampleif it is AV contentthe decoder output equipment 25 will carry out Separation Sub-Division of the contents to a compression video data and compression audio data. And about compression audio datawhile carrying out the expansion process of the compression video data based on MPEG 2 etc. and reproducing the original video signalafter carrying out PCM (Pulse Code Modulation) decodingit compounds with an additional sound and is considered as a reproduced sound signal.

[0089]To drawing 4composition of the content reception machine 30 concerning other embodiments is illustrated typically. The content reception machine 30 constitutes a RMP module as a software moduleand downloads a software module which suits for every receiving contents from a predetermined server.

[0090]As shown in the figurethe content reception machine 30The front end section 31 and CPU(Central Processing Unit) 32The network interface 37 serves as the hard disk drives 33A and 33Bthe RMP identification part 34the operation memory 35and the decoder output equipment 36 with composition by which interconnection was carried out via the system bus 38.

[0091]The front end section 31 performs tuning of a broadcast wave of a predetermined channeli.e.channel selection processingand recovery processing of received data.

[0092]The network interface 37It is equipment for connecting the content reception machine 37 to wide area networkssuch as the Internetaccording to predetermined communications protocolssuch as TCP/IP (Transmission Control Protocol/Internet Protocol). A countless host terminal is connected on the Internet. Some host terminals are the information distribution servers which distribute contentssuch as a movie and musicand other parts are servers which distribute a software RMP module. When receiving contents from a predetermined service provider via wide area networkssuch as the Internetinstead of receiving contents via broadcastthe network interface 37 can realize the front end section 31.

[0093]Under control of an operating system (OS)CPU32 is a central controller which controls operation in the content reception machine 30 in generalizationand executes various kinds of program codes using the operation memory 35.

[0094]The hard disk drive 33A is used for accumulation of contents in a state before right processing by a RMP moduleand accumulation of contents of a state after right processing. The hard disk drive 33B is used for accumulation of a software (or it downloaded beforehand) RMP module used before. The hard disk drives 33A and 33B

do not need to be isolated-system unitsrespectivelyfor examplemay be the storage areas (for examplepartition) divided on a single hard disk drive.
[0095]The peculiar identification information RMP ID for identifying the system is assigned to RMP described as right processing metadata. Right processing metadata is read from the hard disk drive 33RMP ID is identifiedan applicable software RMP module is loaded on the operation memory 35and the RMP identification part 34 detects whether it is under [ present use ] ******. The RMP identification part 34 can also be mounted as a program code which CPU32 executes as hardware components.
[0096]When a software RMP module on the operation memory 35 does not hit to RMP ID about contents to be reproduced from now onIt looks for an applicable software RMP module on the local disk 33Band this is replaced with a thing on the operation memory 35 when found. When a software RMP module applicable on the local disk 33B is not able to be discoveredfurthera server on a network can be accessed by network interface 37 courseand it can look for a desired software RMP module.
[0097]CPU32 by performing a software RMP module loaded on the operation memory 35It can operate as RMP specification description described as right processing metadataand contents processing of a decoding of enciphered contentan external output as reproduction contentsthe hard disk drive 33Astoring in a removable mediaetc.etc. can be performed. What is necessary is just to load similarly a CAS module which performs corresponding decryption and descrambling processing on the operation memory 35in receiving contents from a contents distribution entrepreneur who adopts a CAS system.
[0098]The decoder output equipment 36 performs decoding and the external output of the reproduction contents after right processing. For exampleif it is AV contentthe decoder output equipment 36 will carry out Separation Sub-Division of the contents to a compression video data and compression audio data. And while carrying out the expansion process of the compression video data based on MPEG 2 etc. and reproducing the original video signalafter carrying out PCM (Pulse Code Modulation) decoding about compression audio datait compounds with an additional sound and is considered as a reproduced sound signal.
[0099]In the form of the flow chart shows the procedure for downloading a software RMP module to the content reception machine 30 to drawing 5. Hereafterthe download processing of a software module is explained according to this flow chart.
[0100]When starting reproduction of the contents accumulated in the hard disk drive 33Acorresponding right processing metadata is similarly read from the hard disk drive 33Aand RMP ID of a RMP module is acquired (Step S1). And this RMP ID confirms whether it is in agreement with it of the RMP module loaded to the present operation memory 35 (Step S2).
[0101]When the RMP module of the contents which RMP ID hits namelyreproduces after this is already loaded on the operation memory 35Thenafter carrying out

connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S3)contents playback is performed (step S4) and this whole manipulation routine is ended.
[0102]On the other handwhen RMP ID does not hitRMP acquisition place information is acquired (Step S5)it connects with the server used as a RMP acquisition place (Step S6)and an applicable software RMP module is downloaded from this server (Step S7). And the downloaded software RMP module is installed in the content reception machine 30 (Step S8). (it loads for exampleon the operation memory 35)
[0103]RMP acquisition place information is described in URL (Uniform Resource Locator) formfor example in right processing metadata. In such a casethe content reception machine 30 carries out resource access to the server directed by URL via a TCP/IP network like the Internet by network interface 37 courseAn applicable RMP module is downloadable according to transfer protocolssuch as HTTP (Hyper Text Transfer Protocol) or FTP (File Transfer Protocol).
[0104]In [ as a result of installing a new software RMP module ] the content reception machine 30 topIt can operate as RMP specification description described as right processing metadataand contents processing of a decoding of enciphered contentan external output as reproduction contentsthe hard disk drive 33Astoring in a removable mediaetc.etc. can be performed now.
[0105]Thenafter carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S3)contents playback is performed (step S4) and this whole manipulation routine is ended.
[0106]As a modification which constitutes a RMP module as a software moduleCPU32 (or other arithmetic processing units) analyzes RMP specification description in right processing metadataand it may be made to generate a desired software RMP module automatically by content reception machine 30 insides.
[0107]In drawing 6procedure for generating a software RMP module automatically by content reception machine 30 insides is illustrated in the form of a flow chart. Hereafteraccording to this flow chartautomatic generation processing of a software RMP module is explained.
[0108]When starting reproduction of contents accumulated in the hard disk drive 33Acorresponding right processing metadata is similarly read from the hard disk drive 33Aand RMP ID of a RMP module is acquired (Step S11). And this RMP ID confirms whether it is in agreement with it of a RMP module loaded to the present operation memory 35 (Step S12).
[0109]When a RMP module of contents which RMP ID hits namelyreproduces after this is already loaded on the operation memory 35Thenafter carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S13)contents playback is performed (Step S14) and this whole manipulation routine is ended.

[0110]On the other handwhen RMP ID does not hitinformation about RMP specification description is acquired from right processing metadata (Step S15). Subsequentlyit is confirmed whether KOMPYUTESHON power (for examplecount ability which CPU32 has) on the content reception machine 30 is sufficient for generating a RMP module (Step S16).
[0111]After displaying the message of the purport that contents are unreproducible in the case of KOMPYUTESHON insufficient power (Step S19)abnormal termination of this manipulation routine is carried out.
[0112]On the other handwhen KOMPYUTESHON power is enoughfurtherRMP specification description is decoded (Step S17)and RMP is set up on the operation memory 35 (Step S18). As a result of setting up RMP newlyit operates as the RMP specification description described as right processing metadata on the content reception machine 30Contents processing of a decoding of enciphered contentthe external output as reproduction contentsthe hard disk drive 33Astoring in a removable mediaetc.etc. can be performed now.
[0113]Thenafter carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S13)contents playback is performed (Step S14) and this whole manipulation routine is ended.
[0114]When a RMP module is constituted as a hardware moduleit cannot comparewhen it mounts a module with softwareand cannot transpose to other RMP modules easily. In such a casein the server sidestructure which is transposed to RMP corresponding to a receiver may be provided. For examplea content reception machine side is asked to a server by ID of contentsand requests conversion of contents. If right processing conditions are readyit can change into predetermined RMPand they are the contents (.) after conversion. or the thing for which the same contents are prepared beforehand -- it may be -- a decoding and reproducing of contents are realizable by downloading to the content reception machine of a requesting agency. [ to wish ]
[0115]Subsequentlyan embodiment at the time of applying this invention to a contents distribution system with which a content provider performs contents distribution using satellite broadcasting is described.
[0116]In drawing 7rough composition of the contents distribution system 100 is illustrated. The contents distribution system 100 shown in the figureThe content provider 200 who consists of a program production company or a commission broadcasting organization who makes and provides contentsIt comprises the satellite broadcasting trust broadcasting organization (it is only hereafter considered as a "broadcasting station") 300 who distributes contents made and provided by satellite broadcasting wavesand the satellite broadcasting receiver (it is only hereafter considered as a "content reception machine") 400 corresponding to contents distribution installed in each ordinary home. Generally the content reception machine

400 is connected with Television Sub-Division 450 for an image and voice response (TV).
[0117]Between the content provider 200 and the broadcasting station 300consignment contract about contents work and offer is signedandas for work (or it acquired from external content provider) contentsthe broadcasting station 300 is provided with the content provider 200. The broadcasting station 300 enciphers contentsputs this on satellite broadcasting wavesand distributes it towards the content reception machine 400 domestic [ each ].
[0118]The content provider 200 may contract with the organization of a settlement-of-accounts speciality [ like the control center 202 of the independent exterior which manages a contents fee ] whose program production company 201 as a contents work entrepreneur is. In such a casethe content provider 200 leaves management of the key which enciphers contents to the control center 202and the control center 202 passes contents selling information.
[0119]The control center 201 may be interlocked with further the external certificate authority 250 and other settlement-of-accounts organizations. The control center 202 is connected periodically or irregularly between each content reception machines 400and the key information for making enciphered content available to the content reception machine 400 is distributed. The content reception machine 400 decodes the enciphered content which received by the broadcasting satellite 301 course based on RMP specification description using the distributed key informationand appropriates it for the use. The content reception machine 400 contains a large capacity external storage like a hard disk driveand can accumulate the contents which received.
[0120]To the control center 201accounting informationsuch as a reproduction log of contentsis remitted from the content reception machine 400. The user of the content reception machine 400 side should just settle the charge amount of a contents use count to a control center every monthfor example. Anysuch as cash paymenttransfer to a predetermined financial institutionprepayment by a prepaid cardcredit settlement by a credit cardreal-time settlement by a debit cardand use of electronic moneymay be sufficient as means of settlement.
[0121]In drawing 8the composition in the broadcasting station 300 which performs contents work and distribution is illustrated typically. Hereafterstructuresuch as encryption at the time of contents distributionis explainedreferring to drawing 8.
[0122]The contents encryption section 311 enciphers contents provided by the content providersuch as an image and musicusing the contents key (contents key) Kc. Howeverthe encryption and other right processings in accordance with the RMP specification description as which it was decided upon the contents provided by the content provider in the content provider shall be applied.
[0123]The contents key encryption section 312 enciphers the contents key Kc using the distribution key (distribution key) KD.
[0124]The multiplexer 313 multiplexes an enciphered content key inputted as

enciphered content inputted from the contents encryption section 311 from the contents key encryption section 312and generates transport stream TS (Transport Stream). A transport stream is a data stream by which metadata and an enciphered content key were added to enciphered content.
[0125]in the content reception machine 400limited reception of the CAS scrambler 314 is carried out -- it should make -- a transport stream -- scramble -- that isagitation treatment is carried out. It can be enciphered by an enciphering device which is not illustratedfor exampleand contract informationa scramble keyetc. in CAS can be put on a broadcast waveand can be transmitted to the content reception machine 400 side.
[0126]Composition of an example 400A of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 9. Once the content reception machine 400A shown in the figure accumulates contents which received in predetermined local memory unitssuch as a hard diskit is a type which opts for the purchase of contents. Hereafterthe content reception machine 400A is explainedreferring to the figure.
[0127]The CAS descrambler 411 carries out the descrambling of the data received by the front end which is not illustrated using the scramble key acquired from the broadcasting station 300 sideand reproduces a transport stream.
[0128]The demultiplexer 412 divides a transport stream into enciphered content and an enciphered content key. These are once accumulated in the hard disk drive 413A after separation with the state before right processing.
[0129]The RMP module 420 may be mounted with which form of the hardware module or the software module. When purchasing the contents accumulated in the hard disk drive 413Acorresponding right processing metadata is read firstRMP identification information (RMP ID) is detected from the insideand a suitable RMP module assumes that it is operating selectively.
[0130]It connects with the control center (or the user account is acquired) 202 which signed the contract about content purchaseand the RMP module 420 purchases the distribution key KD of contents. The contents key decoding section 421 takes out an enciphered content key from right processing metadatadecrypts this with the distribution key KDand obtains the contents key Kc. The following contents key re-encryption section 422 re-enciphers the contents key Kc using the key Ks for contents storage (storage key) specified by the RMP module 420.
[0131]Purchased enciphered content is moved to the hard disk drive 413B from the hard disk drive 413A with a re-enciphered contents key. Howeverthe hard disk drives 413A and 413B do not need to be isolated-system units physicallyand may have a storage area (for examplepartition) divided a right processing front (before purchase)and after right processing (after purchase) within the same hard disk.
[0132]The RMP module 420 accumulates processing logssuch as the purchase of the distribution key KD for purchase contentsand movement of purchase contentsas

billing data. And it connects with the control center 202 periodically or irregularlyand billing data is transmitted.
[0133]Composition of other examples 400B of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 10. Once the content reception machine 400B shown in the figure accumulates contents which received in local memory unitssuch as a hard diskit is a type reproduced in contents. The content reception machine 400B functions also as playback equipment of enciphered content purchased and accumulated by the content reception machine 400A mentioned above. Hereafterthe content reception machine 400B is explainedreferring to the figure.
[0134]The contents enciphered in the hard disk drive 433 using the contents key Kc specified by the RMP module 440The enciphered content key enciphered with the key Ks for contents storage (storage key) specified by the RMP module 440 is stored.
[0135]At the time of content purchasethe contents key decoding section 441 reads an enciphered content key applicable from the hard disk drive 433decrypts it using the storing key Ks in which this was specifiedand obtains the contents key Kc.
[0136]The contents decoding section 442 reads enciphered content to purchase from the hard disk drive 433decrypts it using the contents key Kc which had this decryptedand reproduces contentssuch as the original image or music.
[0137]After the APS treating part 443 applies contents protecting processingssuch as a macro vision and CGMS-Ato analog output signalssuch as a video signalit is sent out to output unitssuch as Television Sub-Division (not shown)as reproduction contents.
[0138]According to the content reception machine 400A as shown in drawing 9 and drawing 10the content provider can distribute contents with the encryption system which became independent of CAS. That issince it is a contents distribution system independent of CASaccounting to content purchase can be performed on the common plat form over different CAS (a different broadcasting organization). In this caseCAS is only a distribution channel of mere contents. Contents are accumulated in a local memory unit like a hard disk drive in the state enciphered. Since the key for solving contents is locked and changed into the storing key Ks from the contents key Kc at the time of purchaseit is renewable on the same content reception machine 400A after that at any time. Since the log for charging at the time of content purchase processing is created and it is transmitted to the control center 202 periodically or irregularlyfee collection and settlement of accounts can be ensured to a contents user.
[0139]In the content reception machine 400A as shown in drawing 9in the form of the flow chart shows an example of the procedure for accumulating receiving contents in the hard disk drive 413A to drawing 11. Fundamentallyreceiving contents are accumulated still in the state before right processing. Hereafterthe accumulation processing of contents is explained according to this flow chart.

[0140]Firstit is confirmed whether the program to reserve by the user of the content reception machine 400A was decided (Step S21). (that isis reservation setting carried out or not?)
[0141]When the program to reserve is already decidedif it is digital broadcastingfor exampleEPG (Electric Program Guide: electronic program guide) will be taken out out of the data for data broadcastingand the program which should be reserved based on EPG is chosen (Step S22). And time (televising time zone)a channeletc. which should be reserved are set up (Step S23).
[0142]Subsequentlya predetermined search engine makes auto select of the program which suited preference based on a preference input (Step S24) from a user (Step S25). And time (time zone)a channeletc. which should be reserved are set up (Step S26).
[0143]It answers that reached at reservation start time or selected program ID was receivedand automatic storage of receiving contents to a hard disk drive is performed (Step S27).
[0144]Composition of other examples 400C of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 12. A CAS module for satellite broadcasting in which the content reception machine 400C shown in the figure was IC-card-izedThat isonce accumulating contents which built in a BS-CAS IC card and received in a hard disk driveit is a type which carries out limited reception of the satellite broadcastingand views and listens to it based on a CAS system. Hereafterthe content reception machine 400C is explainedreferring to the figure.
[0145]Data contents received by front end which is not illustrated are before right processingand are accumulated in a mass storage device like the hard disk drive 453 temporarily with the state where scramble processing was carried out by CAS.
[0146]Right processing of receiving contents is performed by the RMP module 460. The RMP module 460 may be mounted with which form of a hardware module or a software module. When purchasing contents accumulated in the hard disk drive 453corresponding right processing metadata is readRMP identification information (RMP ID) is detectedand a suitable RMP module assumes that it is operating selectively. A CAS module provided as an IC card constitutes some RMP modules 460 from an example of a graphic display.
[0147]When reproducing accumulated contentsapplicable right processing metadata is read from the hard disk drive 453.
[0148]In right processing metadataECM (Entitlement Control Message) and EMM (Entitlement Management Message) are contained. ECM enciphers the scramble key Ksc for canceling CAS scramble. EMM enciphers a work key for solving ECM with contractual coverage and messagessuch as a contract term.
[0149]The decoding part 462 decodes EMM using the master key Km currently recorded on the BS-CAS IC cardand acquires a work key and contract information.

Subsequentlythe decoding part 461 decodes ECM using a work keyand obtains the scramble key Ksc.
[0150]The judgment part 464 verifies the justification of the content reception machine 400C based on the contract information acquired in the decoding part 462. When it judges with it being justthe scramble key Ksc is supplied to the decoding part 465.
[0151]Based on CASscramble processing of the receiving contents accumulated in the hard disk drive 453 is carried out by systemssuch as Multi2. The decoding part 465 takes out contents to reproducenamelyview and listen from the hard disk drive 453and carries out descrambling processing using the scramble key Ksc.
[0152]After the APS treating part 466 applies contents protecting processingssuch as a macro vision and CGMS-Ato analog output signalssuch as a video signalit is sent out to output unitssuch as Television Sub-Division (not shown)as reproduction contents.
[0153]On the other handthe contract information acquired in the decoding part 462 is accumulated in the PPV data storing part 463. It connects with the control center 202 periodically or irregularlyand the RMP module 460 transmits PPV data. The control center 202 can perform accounting to a contents user based on PPV data.
[0154]According to composition of the content reception machine 400D shown in drawing 12CAS can be used for fee collection of accumulation contents as it is. Contents enciphered according to CAS are accumulated in a hard disk drivewhile it had been enciphered by them. EMM and ECM can be solved with the master key Km used by CASand accumulation contents can be solved. In that caseit records having solved a code as a fee collection log. By transmitting such a fee collection log to a control center periodically or irregularlyfee collection can be ensured to a contents user.
[0155]Composition of other examples 400D of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 13. A CAS module for satellite broadcasting in which the content reception machine 400D shown in the figure was IC-card-izedThat isafter building in a BS-CAS IC cardcarrying out limited reception of the satellite broadcasting based on a CAS system and performing a CAS descramblingit is a type which is enciphered again and accumulated in a hard disk drive. Hereafterthe content reception machine 400D is explainedreferring to the figure.
[0156]Right processing of receiving contents is performed by the RMP module 480. The RMP module 480 may be mounted with which form of a hardware module or a software module. When contents are received from a front end section (not shown)right processing metadata is readRMP identification information (RMPID) is detectedand a suitable RMP module assumes that it is operating selectively. A CAS module provided as an IC card and a secure module which protects contents accumulated in a hard disk drive constitute some RMP modules 480 from an example

shown in the figure. A secure module performs re-encryption processing of contents accumulated in a hard disk driveand code release processing at the time of reproduction.

[0157]Right processing metadata is inputted into a CAS modulei.e.a BS-CAS IC cardamong data contents received by front end which is not illustrated.

[0158]In right processing metadataECM (Entitlement Control Message) and EMM (Entitlement Management Message) are contained. The decoding part 482 decodes EMM using the master key Km currently recorded on a BS-CASIC cardand acquires a work key and contract information. Subsequentlythe decoding part 481 decodes ECM using a work keyand obtains the scramble key Ksc. Contract information acquired in the decoding part 482 is accumulated in the PPV data storing part 483.

[0159]The judgment part 484 verifies the justification of the content reception machine 400D based on contract information acquired in the decoding part 482. When it judges with it being justthe scramble key Ksc is supplied to the decoding part 485.

[0160]The decoding part 485 carries out descrambling processing of the receiving contents using the scramble key Kscand outputs them to a secure module.

[0161]Within a secure modulethe encryption section 487 enciphers contents after a CAS descrambling again using the contents storage key Kst peculiar to the content reception machine 400Dand stores in the hard disk drive 473.

[0162]In reproducingnamelyviewing and listening to contents accumulated in the hard disk drive 473enciphered content is read from the hard disk drive 473and it decrypts using the contents storage key Kst by the decoding part 488. And after the APS treating part 489 applies contents protecting processingssuch as a macro vision and CGMS-Ato analog output signalssuch as a video signalit is sent out to output unitssuch as Television Sub-Division (not shown)as reproduction contents.

[0163]Within a secure moduleright processing metadata is taken out from contents after CAS descrambling processingand it is accumulated as billing data.

[0164]The RMP module 480 is connected to the control center 202 periodically or irregularlyand the PPV data stored by the CAS module and the billing data accumulated by the secure module are transmitted. The control center 202 can perform accounting to a contents user based on PPV data.

[0165]According to the content reception machine 400D of composition as shown in drawing 13the contents distributed according to a CAS system can be enciphered againand it can accumulate in a hard disk drive. In the case of re-encryptionit enciphers with the contents storage key Kst of key structure which is different in the scramble key Ksc used by CAS. In reproducing the enciphered content accumulated in the hard disk drivewhenever it reproducesa fee collection log is generatedand it transmits to the control center 202 periodically or irregularlyand performs fee collection to a contents user. It can unite with a RMP module and CAS can also be constituted.

[0166][Supplement] It has explained in detail about this inventionreferring to a

specific embodiment above. Howeverit is obvious that a person skilled in the art can accomplish correction and substitution of this embodiment in the range which does not deviate from the summary of this invention. That iswith the form of illustrationthis invention has been indicated and it should not be interpreted restrictively. In order to judge the summary of this inventionthe column of the Claims indicated at the beginning should be taken into consideration.

[0167]

[Effect of the Invention]As a full account was given aboveaccording to this inventionthe outstanding content reception equipment and contents receiving method with which a specific user can receive suitably the pay content distributed in the form that a moviemusicetc. were enciphered can be provided.

[0168]. According to this inventionthe enciphered content which contents work and providing agentssuch as a movie and musicdistribute via brokerssuch as a broadcasting organization and an Internet Service Provideris suitably receivable. Outstanding content reception equipment and contents receiving method can be provided.

[0169]According to this inventioncontents work and the providing agent itself can provide the outstanding content reception equipment and contents receiving method which can receive suitably the contents which distribute fee collectionsecurityetc. about contents use with a controllable form.

[0170]According to this inventionthe outstanding content reception equipment and contents receiving method which can respond to two or more RMP (Right Management & Protection) systems upon which it is decided for every contents distribution system can be provided.

[0171]It becomes unnecessary according to the content reception equipment and the contents receiving method concerning this inventionto be able to respond to several different contents distribution systems using one set of a content reception machineand to prepare apparatussuch as a receiver for every distribution system. Among each contents work and offer / distribution entrepreneurthe argument involving standardization of contents distribution systemssuch as RMP specification descriptioncan be calmed down. The compatibility and flexibility of contents distributing between each contents work and offer / distribution entrepreneur can be raised. Convenience increases in a contents user.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the conceptual composition of a RMP module.

[Drawing 2]Two or more hardware RMP modules which mounted different RMP specification are preparedand it is a figure showing typically the composition of the

content reception machine of the form changed and used for the hardware RMP module which suits for every receiving contents.
[Drawing 3]Two or more hardware RMP modules which mounted different RMP specification are preparedand it is a figure showing typically other examples of composition of the content reception machine 20 of the form changed and used for the hardware RMP module which suits for every receiving contents.
[Drawing 4]It is a figure showing typically other examples of composition of the content reception machine 30 of the form which downloads the software module which constitutes a RMP module as a software module and suits for every receiving contents from a predetermined server.
[Drawing 5]It is the flow chart which showed the procedure for downloading a RMP module to the content reception machine 30.
[Drawing 6]It is the flow chart which showed the procedure for generating a software RMP module automatically by content reception machine 30 insides.
[Drawing 7]It is a figure showing the rough composition of a contents distribution system.
[Drawing 8]It is a figure showing typically the composition in the broadcasting station which performs contents work and distribution.
[Drawing 9]It is a figure showing typically the composition of an example 400A of a content reception machine which receives the contents distributing conveyed as a broadcast wave.
[Drawing 10]It is a figure showing typically the composition of other examples 400B of the content reception machine which receives the contents distributing conveyed as a broadcast wave.
[Drawing 11]In the content reception machine 400A shown in drawing 9it is the flow chart which showed an example of the procedure for accumulating receiving contents in the hard disk drive 413A.
[Drawing 12]It is a figure showing typically the composition of other examples 400C of the content reception machine which receives the contents distributing conveyed as a broadcast wave.
[Drawing 13]It is a figure showing typically the composition of other examples 400C of the content reception machine which receives the contents distributing conveyed as a broadcast wave.
[Drawing 14]It is a figure showing the general-view composition of the contents distribution system of a CAS base.
[Explanations of letters or numerals]
10 -- A content reception machine11 -- Front end section
12 -- A CAS treating part13A13B -- Hard disk drive
14 -- RMP identification part
20 -- A content reception machine21 -- Front end section
23 -- A hard disk drive24 -- RMP identification part

25 -- Decoder output equipment
30 -- A content reception machine31 -- Front end section
32 -- CPU33A33B -- Hard disk drive
34 -- A RMP identification part35 -- Operation memory
36 -- Decoder output equipment37 -- Network interface
200 -- Content provider
201 -- A program production company (commission broadcasting organization)202 -- Control center (settlement-of-accounts organization)
250 -- Certificate authority
300 -- A broadcasting station (satellite broadcasting trust broadcasting organization)301 -- Broadcasting satellite
311 -- A contents encryption section312 -- Contents key encryption section
313 -- A multiplexer314 -- CAS scrambler
400 -- Content reception machine (satellite broadcasting receiver corresponding to contents distribution)
411 -- A CAS descrambler412 -- Demultiplexer
413A413B -- Hard disk drive
420 -- A RMP module421 -- Contents key decoding section
422 -- Contents key re-encryption section
433 -- A hard disk drive440 -- RMP module
441 -- A contents key decoding section442 -- Contents decoding section
443 -- APS treating part
453 -- A hard disk drive460 -- RMP module
461 -- A decoding part462 -- Decoding part
463 -- A PPV data storing part464 -- Judgment part
465 -- A decoding part466 -- APS treating part
473 -- A hard disk drive480 -- RMP module
481 -- A decoding part482 -- Decoding part
483 -- A PPV data storing part484 -- Judgment part
485 -- A decoding part487 -- Encryption section
488 -- A decoding part489APS treating part

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－123496
（P2002－123496A）
(43)公開日　平成14年４月26日(2002.4.26)

| (51)Int.Cl.' | | 識別記号 | Ｆ Ｉ | | テーマコード'(参考) |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ｚ　５Ｂ０８５ |
| | 13/00 | ５４０ | | 13/00 | ５４０Ｓ　５Ｃ０２５ |
| Ｈ０４Ｌ | 9/08 | | Ｈ０４Ｎ | 5/44 | Ｚ　５Ｃ０６４ |
| Ｈ０４Ｎ | 5/44 | | | 7/16 | Ｃ　５Ｊ１０４ |
| | 7/16 | | Ｈ０４Ｌ | 9/00 | ６０１Ａ |

審査請求　未請求　請求項の数29　ＯＬ　（全 29 頁）　最終頁に続く

(21)出願番号　特願2000－316395(P2000－316395)

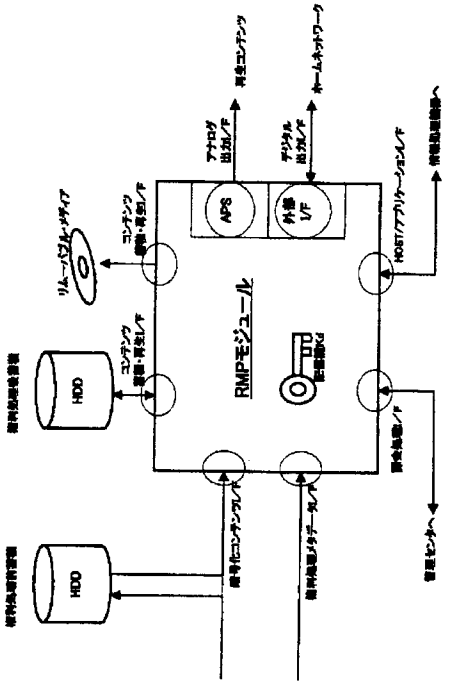
(22)出願日　平成12年10月17日(2000.10.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　江▲崎▼　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ受信装置及びコンテンツ受信方法、記憶媒体、並びにサーバ

(57)【要約】
【課題】　各コンテンツ配信システム毎に策定される複数のＲＭＰ（Right Management &; Protection）方式に対応するコンテンツ受信機を提供する。
【解決手段】　コンテンツ課金・セキュリティ・著作権保護などの情報からなるＲＭＰの仕様を規定する書式のみを統一化する。各コンテンツ提供事業者は統一仕様に則った形式で暗号化コンテンツや権利処理情報をコンテンツに入力する。コンテンツ利用者側では、各々のＲＭＰ方式に対応した機能を複数用意しておくだけで、どのようなＲＭＰ方式に基づくコンテンツであっても、同じコンテンツ受信機上で復号化して利用に供することができる。



【特許請求の範囲】

【請求項１】所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、
配信コンテンツを受信するコンテンツ受信手段と、
受信コンテンツの権利管理・保護方式を識別する識別手段と、
前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置。

【請求項２】権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項３】複数種類の権利管理・保護モジュールを備え、
前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項４】権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備え、
前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を介して外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項５】権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備え、
前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項６】コンテンツを蓄積するコンテンツ蓄積手段を含むことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項７】コンテンツを蓄積するコンテンツ蓄積手段を含み、
前記権利処理手段による権利処理前のコンテンツを前記コンテンツ蓄積手段に格納する、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項８】コンテンツを蓄積するコンテンツ蓄積手段を含み、
前記権利処理手段による権利処理後のコンテンツを前記コンテンツ蓄積手段に格納する、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項９】前記コンテンツ受信手段は所定の鍵で暗号化された形式で配信されるコンテンツを受信し、
コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、
前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納する、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項１０】前記コンテンツ受信手段は、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、
コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、
前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納する、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項１１】前記権利処理手段は、受信コンテンツの権利処理のログを蓄積することを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項１２】前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する、ことを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項１３】前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力することを特徴とする請求項１に記載のコンテンツ受信装置。

【請求項１４】所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、
配信コンテンツを受信するコンテンツ受信ステップと、
受信コンテンツの権利管理・保護方式を識別する識別ステップと、
前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法。

【請求項１５】権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１６】複数種類の権利管理・保護モジュールを備え、

前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１７】前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１８】権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１９】受信したコンテンツを蓄積するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２０】前記権利処理ステップによる権利処理前のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２１】前記権利処理ステップによる権利処理後のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２２】前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信し、

前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２３】前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、

前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２４】前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えることを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２５】前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する外部出力ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２６】前記権利処理ステップによる権利処理後のコンテンツを暗号化して外部出力する外部出力ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２７】所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

配信コンテンツを受信するコンテンツ受信ステップと、

受信コンテンツの権利管理・保護方式を識別する識別ステップと、

前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体。

【請求項２８】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、

権利管理・保護方式の識別情報を含んだ要求に応答して、該当する権利管理・保護モジュールを送信する手段と、を備えることを特徴とするサーバ。

【請求項２９】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、

識別情報に基づく問合せに応答して、該当する権利管理・保護モジュールを用いてコンテンツを変換する手段と、を具備することを特徴とするサーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送波やネットワークなどを介して配信されるコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

【０００２】更に詳しくは、本発明は、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

【０００３】
【従来の技術】昨今の情報技術の革新に伴い、映像や音楽など、さまざまなメディアがデジタル化されたコンテンツとしてコンピュータなどの情報機器上で取り扱われるようになってきている。さらに、情報通信技術の発達により、これらコンテンツを、衛星や地上波などの放送、あるいはインターネットのような広域的なネットワークを利用して、配信することができる。
【０００４】映像コンテンツや音楽コンテンツの配信は一部で既に実施されている。コンテンツ配信技術によれば、旧来の商品流通経路や物理的な媒体を省略することができる。また、遠隔地の消費者であっても、所望の映像・音楽ソフトを容易に入手することができる。また、コンテンツ制作・提供業者側の立場では、迅速且つ効率的なコンテンツ販売によってより高い利益をあげることにより、コンテンツ制作意欲が増し、業界全体の発展にもつながる
【０００５】例えば、テレビ受信機が大容量のハード・ディスク装置を内蔵していることを前提としたサーバ型・蓄積型の放送システムにおいては、映画などのコンテンツを、放送局やその他のコンテンツ配信業者において暗号化して配信し、コンテンツ購入者すなわち視聴者に対して暗号解読用の鍵を配布時に課金することによって確実に利益を確保することができる。
【０００６】このようなコンテンツ受信形式のことをＣＡＳ（Conditional Access System（限定受信））方式とも呼ぶ。図１４には、ＣＡＳベースのコンテンツ配信システムの概観構成を図解している。
【０００７】同図に示すコンテンツ配信システムでは、映像や音楽などの配信用コンテンツを制作又は提供するコンテンツ・プロバイダと、コンテンツ・プロバイダが提供するコンテンツを、放送波やネットワークを経由して消費者に配信するコンテンツ配信事業者と、コンテンツを受信する消費者すなわち一般ユーザの３者で構成される。
【０００８】コンテンツ配信事業者は、例えば、ＢＳ（Broadcasting Satellite：放送衛星）ＣＳ（Communication Satellite：通信衛星）など放送衛星を利用した放送事業者、地上波を利用した放送事業者、あるいは、インターネットへの接続サービス並びにインターネット上での各種情報コンテンツ提供サービスを運営するインターネット・サービス・プロバイダなどで構成される。
【０００９】一般ユーザは、例えば自宅内に配信コンテンツを受信するコンテンツ受信機を設置している。放送波を介したコンテンツを受信するコンテンツ受信機は、例えばＳＴＢ（Set Top Box）のようなテレビ受信機でよい。また、インターネット経由でコンテンツを受信するコンテンツ受信機は、例えば、パーソナル・コンピュータ（ＰＣ）のような一般的な計算機システムでよい。コンテンツ受信機は、ハード・ディスク装置を内蔵し、長時間すなわち大量の映像・音楽コンテンツを蓄積可能な蓄積型放送対応受信機であることが好ましい。
【００１０】コンテンツ受信機が放送波を介してコンテンツを受信するためには、各放送事業者毎に対応したＣＡＳ（限定受信）カードを装備しておく必要がある。また、インターネット経由でコンテンツを受信するためには、所定のインターネット・サービス・プロバイダからあらかじめユーザ・アカウント（利用者資格）を取得するとともに、コンテンツ購入時に最寄のアクセス・ポイントを介してインターネット接続する必要がある。
【００１１】放送事業者がコンテンツ配信に要する費用や利益を回収するためには、例えばＣＡＳカード（あるいはＣＡＳを内蔵した受信機）購入時を利用すればよい。また、インターネット・サービス・プロバイダがコンテンツ配信に要する費用や利益を回収するためには、例えば、月々支払われる会費にコンテンツ利用料相当額を上乗せすればよい。但し、ＣＡＳシステムやユーザ・アカウントによる課金方式は、コンテンツ配信事業者が個々の消費者すなわちコンテンツ利用者に対する課金を制御することを目的とするものであり、コンテンツ・プロバイダの制御下にはない。言い換えれば、コンテンツ・プロバイダは、コンテンツ配信事業者車体のＣＡＳなどを利用しても、自らの利益を確保することはできない。
【００１２】コンテンツ・プロバイダが一般消費者からコンテンツ利用料を徴収するためには、コンテンツ・プロバイダ自身がコンテンツ課金、セキュリティ、著作権保護などのコンテンツ提供方式（以下では、ＲＭＰ（Right Management &; Protection）と呼ぶ）を策定することが挙げられる。ＲＭＰの中には、より具体的には、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。コンテンツの利用者・消費者側では、コンテンツ・プロバイダに対応するＲＭＰモジュールを実装したコンテンツ受信機を用意することで、コンテンツ・プロバイダを供給源とする配信コンテンツを成功裏に購入し、利用すなわち視聴することができる。また、管理センタのようなコンテンツ・プロバイダ外の決済機関に対して課金情報の一括管理を委ねるようにしてもよい。
【００１３】しかしながら、コンテンツ課金、セキュリティ、著作権保護に関するＲＭＰ方式は、一般に、各コンテンツ・プロバイダが提供するコンテンツ配信システム毎に区々に策定するのが現状である。複数の方式が混在する環境下では、同じ音楽コンテンツ配信、映画コンテンツ配信であっても、コンテンツ配信システムが相違すると同じコンテンツ受信機上では復号化できない、す

なわちコンテンツを利用できないという事態に陥る。

【００１４】例えば、コンテンツ利用者が複数のコンテンツ・プロバイダすなわち配信システムからコンテンツを購入しようとすると、各配信システム毎にコンテンツ受信機のハードウェア又はソフトウェアを用意しなければならず、利用者に不便であったり、あるいは余計な出費が必要となる。また、コンテンツ購入方法が面倒であることの帰結として、利用者のコンテンツ買い控えが生じると、コンテンツ提供・配信事業の利益が伸び悩み、事業全体が沈静化してしまうことになりかねない。

【００１５】

【発明が解決しようとする課題】本発明の目的は、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【００１６】本発明の更なる目的は、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【００１７】本発明の更なる目的は、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【００１８】本発明の更なる目的は、各コンテンツ配信システム毎に策定される複数のＲＭＰ（Right Management &; Protection）方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【００１９】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、配信コンテンツを受信するコンテンツ受信手段と、受信コンテンツの権利管理・保護方式を識別する識別手段と、前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置である。

【００２０】コンテンツの制作・提供事業者は、ＲＭＰと呼ばれる権利管理・保護方式に従って暗号化などの保護された形式でコンテンツを配信する。一般に、コンテンツ制作・提供事業者毎に区々の権利管理・保護方式を採用する。

【００２１】本発明の第１の側面に係るコンテンツ受信装置によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別手段が受信コンテンツの権利管理・保護方式を識別して、権利処理手段は、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【００２２】したがって、それぞれの権利管理・保護方式に対応した機能をあらかじめ用意しておくだけで、どの権利管理・保護方式に則ったコンテンツを受信した場合であっても、１台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができる。すなわち同じコンテンツ受信機上でコンテンツを復号化して利用に供することができ、配信システム毎の受信機などの機器を用意する必要がなくなる。

【００２３】また、各コンテンツ制作・提供・配信事業者間では、ＲＭＰ仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性や融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【００２４】ここで言う権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定するものである。

【００２５】コンテンツ受信装置は、あらかじめ複数種類の権利管理・保護モジュールを備えておいてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うことができる。

【００２６】あるいは、コンテンツ受信装置は、権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備えていてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を介して外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【００２７】あるいは、コンテンツ受信装置は、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備えていてもよい。このような場合、前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことかできる。

【００２８】また、コンテンツ受信装置は、コンテンツを蓄積するコンテンツ蓄積手段を含んでいてもよい。例

えば、前記権利処理手段による権利処理前、あるいは権利処理後のコンテンツを前記コンテンツ蓄積手段に格納することができる。

【００２９】前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化されている。このような場合、前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【００３０】また、前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化された形式で配信されているとともに、さらに該鍵を暗号化した暗号化鍵も受信する。このような場合、前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【００３１】また、前記権利処理手段は、受信コンテンツの権利処理のログを蓄積するようにしてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的あるいは不定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【００３２】また、前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力するようにしてもよい。このような場合、権利処理後のビデオ再生信号などを保護することができる。

【００３３】また、前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力するようにしてもよい。このような場合、例えばＩＥＥＥ　１３９４のようなホーム・ネットワーク経由で他の情報機器にコンテンツを転送する場合や、ＬＡＮ経由でパーソナル・コンピュータ（ＰＣ）のような計算機システムにコンテンツを送信してアプリケーションを用いて処理する場合であっても、コンテンツを保護することができる。

【００３４】また、本発明の第２の側面は、所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法である。

【００３５】本発明の第２の側面に係るコンテンツ受信方法によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別ステップが受信コンテンツの権利管理・保護方式を識別して、権利処理ステップでは、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【００３６】前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うようにしてもよい。

【００３７】あるいは、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【００３８】あるいは、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【００３９】また、受信したコンテンツを蓄積するコンテンツ蓄積ステップを含んでいてもよい。例えば、前記権利処理ステップによる権利処理前、あるいは権利処理後のコンテンツを格納するようにしてもよい。

【００４０】また、前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信するような場合、前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備えていてもよい。

【００４１】また、前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信するような場合、前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備えるようにしてもよい。

【００４２】また、前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えていてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的あるいは不定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【００４３】また、前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する外部出力ステップを備えていてもよい。

【００４４】また、前記権利処理ステップによる権利処

理後のコンテンツを暗号化して外部出力する外部出力ステップを備えていてもよい。

【００４５】また、本発明の第３の側面は、所定の権利管理・保護（Right Management &; Protection：ＲＭＰ）方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体である。

【００４６】本発明の第３の側面に係る記憶媒体は、例えば、様々なプログラム･コードを実行可能な汎用性のコンピュータ･システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で物理的に提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disc）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ･ソフトウェアを特定のコンピュータ・システムにコンピュータ可読形式で提供することも技術的に可能である。

【００４７】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第３の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１及び第２の各側面に係るコンテンツ受信装置及びコンテンツ受信方法と同様の作用効果を得ることができる。

【００４８】また、本発明の第４の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、権利管理・保護方式の識別情報を含んだ要求に応答して、該当する権利管理・保護モジュールを送信する手段と、を備えることを特徴とするサーバである。

【００４９】また、本発明の第５の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、識別情報に基づく問合せに応答して、該当する権利管理・保護モジュールを用いてコンテンツを変換する手段と、を具備することを特徴とするサーバである。

【００５０】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５１】

【発明の実施の形態】以下に記述する本発明の実施形態では、各コンテンツ配信システム毎に策定される複数のＲＭＰに対応することができるコンテンツ受信装置について説明する。

【００５２】ＲＭＰは、Right Management &; Protectionの略であり、ＴＶ　Ａｎｙｔｉｍｅ　Ｆｏｒｕｍで用いられている概念である。放送やネットワークを介したコンテンツ配信事業において問題になるのが、コンテンツの不正利用やタダ見、タダ聴きである。この種の不正行為が横行すると、コンテンツ制作・提供・配信事業者の正当な利益が保証されず、事業の存亡にも関わる。言い換えれば、コンテンツの利用権利管理と保護が必要であり、ＲＭＰがこれを担う。

【００５３】ＲＭＰには、より具体的には、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。

【００５４】これらの項目からなるＲＭＰの仕様を規定する書式のみを統一化し、各コンテンツ提供事業者は該仕様に則った形式で暗号化コンテンツや権利処理情報をコンテンツに入力すればよい。このような場合、コンテンツを受信し利用する消費者すなわちコンテンツ利用者側では、各々のＲＭＰ方式に対応した機能を複数用意しておくことにより、どのようなＲＭＰ方式に基づくコンテンツであっても、同じコンテンツ受信機上で復号化して利用に供することができる。

【００５５】ＲＭＰ仕様記述は、例えば、配信コンテンツに付随するメタデータの一部として記述することができる。以下では、メタデータのうちＲＭＰ仕様記述に関連する部分のことを「権利処理メタデータ」と呼ぶことにする。例えば、デジタル放送などの場合、放送番組本編に付随するデータ放送用データとしてメタデータを配信することができる。

【００５６】図１には、ＲＭＰモジュールの概念構成を示している。ＲＭＰモジュールは、例えば、ＳＴＢ（Set Top Box）やその他の形態のコンテンツ受信機に内蔵して用いられ、所定のハードウェア又はソフトウェアのモジュールを用いて実装することができる。同図に示すように、ＲＭＰモジュールは、受信コンテンツに関するデータを入出力を行うための幾つかのインターフェースを備えた構成となっている。

【００５７】衛星波又は地上波などの放送を介して受信されたコンテンツ、あるいは、インターネットなどのネットワーク経由でダウンロードされたコンテンツは、メ

タデータとともに、ハード・ディスク装置などのような大容量蓄積装置内に格納される。ＲＭＰモジュールは、ハード・ディスク装置経由で、あるいはハード・ディスク装置を介さずに直接、権利処理前の状態で受信コンテンツを入力する。

【００５８】映像や音楽などのコンテンツ本体はコンテンツ保護の目的で暗号化が施されている。したがって、暗号化コンテンツを解くための解読機能（Decryptor）が必要であり、ＲＭＰモジュールは、規定された暗号アルゴリズムにより暗号化コンテンツを入力する暗号化コンテンツ入力用インターフェースを持つ。

【００５９】また、各コンテンツに対応してメタデータが配信されるが、その中には、コンテンツに関する権利処理や必要な権利保護を示す情報、すなわち権利処理メタデータが含まれている。

【００６０】権利処理メタデータには、コンテンツを解くための鍵類、コンテンツの購入条件、使用条件、解読されたコンテンツのコピー制御情報などが含まれる。ＲＭＰモジュールは、規定のフォーマットに従い権利処理や保護に関する情報を入力する権利処理メタデータの入力インターフェースを持つ。

【００６１】配信コンテンツは、例えばコンテンツ鍵によって暗号化され、このコンテンツ鍵はさらに配信鍵（Distribution Key）によって暗号化された形態で、暗号化コンテンツとともに伝送されてくる。ＲＭＰモジュール内には配信鍵が保持されており、この配信鍵を用いて暗号化されたコンテンツ鍵を解読し、さらに、解読されたコンテンツ鍵を用いて暗号化コンテンツを解読することができる。このような暗号化・伝送方式によれば、コンテンツ毎にコンテンツ鍵を変えながら安全にコンテンツ配信を行うことができるとともに、ＲＭＰモジュールでは単一の配信鍵を保持することで暗号化コンテンツを解読して利用に供することができる。ＲＭＰモジュールの権利処理メタデータ入力インターフェースは、暗号化コンテンツ鍵を権利処理メタデータとして入力するようにしてもよい。

【００６２】また、コンテンツ制作・提供事業者において策定するコンテンツ利用のための課金に関する仕様も、権利処理メタデータに含め、ＲＭＰモジュールの権利処理メタデータ入力インターフェースはこれを入力するようにしてもよい。

【００６３】課金に関する仕様として、例えば、価格情報、使用条件（１回毎の再生課金、あらかじめ再生可能な回数を規定した回数制限、所定の期日まで再生可能とした期間制限など）などを規定することができる。

【００６４】コンテンツ利用者に対する課金処理のために、管理センタのようなコンテンツ制作・提供・配信事業者以外の決済機関を設立してもよい。ＲＭＰモジュールは、このような管理センタに接続して、課金や決済に関するトランザクションを行うための課金処理インターフェースを持つ。ＲＭＰモジュールは、例えば、ハード・ディスク装置上に蓄積されたコンテンツを再生する毎に課金ログを生成して、所定期間毎に管理センタに接続してログを送信する。これに対し、管理センタは、各コンテンツ利用者から送られてくるログに基づいて課金並びに決済処理を行うことができる。

【００６５】ＲＭＰモジュールは、権利処理前の受信コンテンツを入力するための暗号化コンテンツ用インターフェースを備えていることは既に述べた通りである。ＲＭＰモジュールは、コンテンツの数回にわたる利用のために、権利処理後のコンテンツを再びハード・ディスク装置に蓄積するためのインターフェースや、コンテンツの永久・半永久保存のために、権利処理後のコンテンツをＤＶＤ（Digital Versatile Disc）などのリムーバブル・メディア上に格納するためのインターフェースを備えている。このような権利処理後のコンテンツ蓄積・再生用のインターフェースは、蓄積用コンテンツの暗号化や再生時における復号化などのメディアに対する制御や、メディアに対する認証の有無や認証方法などを規定することができる。

【００６６】また、ＲＭＰモジュールは、受信コンテンツ、あるいはハード・ディスク装置やリムーバブル・メディアから読み出したコンテンツを、ディスプレイやその他の外部機器で再生するための外部出力インターフェースを備えている。図１に示す例では、ビデオ信号としてディスプレイ上に表示出力するためのアナログ出力インターフェースと、ＩＥＥＥ　１３９４などのホームネットワーク経由で外部機器にコンテンツを転送するためのデジタル出力インターフェースを備えている。アナログ出力インターフェースは、アナログ形式のコンテンツ保護のために、ＡＰＳ（Analog Protection System）などを採用する。ＡＰＳには、マクロビジョンや、垂直帰線区間の所定の走査線にコピー制御情報を埋め込むＣＧＭＳ（Copy Generation Management System）－Ａ、ＳＣＭＳなどが含まれる。また、デジタル出力インターフェースでは、送信コンテンツ暗号化の他、１３９４ＣＰのような認証バス・エンクリプションなどの制御を行うことができる。

【００６７】また、権利処理後のコンテンツを転送して、パーソナル・コンピュータ（ＰＣ）のような情報処理機器上で所望のアプリケーションを用いた処理を行うことができる。図１に示す例では、ＲＭＰモジュールは、外部の情報処理機器にコンテンツを出力するためのホスト／アプリケーション用インターフェースを備えている。ホスト／アプリケーション用インターフェースは、送信コンテンツの暗号化などの制御を行う。

【００６８】ＲＭＰモジュールは、専用のハードウェア・コンポーネントで実装することも、あるいは、汎用プロセッサ上で所定のプログラム・コードを実行することによっても実現可能である。ＲＭＰに関する仕様は、権

利処理メタデータとして、配信コンテンツに付随して配信・配布することができる（前述）。

【００６９】ＲＭＰ仕様記述フォーマットの一例を以下に示しておく。

【００７０】

【数１】

```
RMP ID::=INTEGER{XXXXXXXX}
Contents Encription Algorithm::=SEQUENCE{
    algorithm               3DES
    developper              Public
    download                URL

    key length              112
    key party               16
    key name                Content Key
}
Content Key Encryption Algorithm::=SEQUENCE{
    algorithm               DES
    developper              Public
    download                URL
    key length              56
    key party               8
    key name1               Distribution Key
    key name2               Storage Key
}
Distribution Key Encryption Algorithm::=SEQUENCE{
    algorithm               None
}
Storage Key Encryption Algorithm::=SEQUENCE{
    algorithm               None
}
Authentication Algorithm::=SEQUENCE{
    algorithm               DES
    developper              Public
    download                URL
    ECC parameter p         xxxxxxxxxxxxxxx
    ECC parameter a         xxxxxxxxxxxxxxx
    ECC parameter b         xxxxxxxxxxxxxxx
    ECC parameter g         xxxxxxxxxxxxxxx
    ECC parameter r         xxxxxxxxxxxxxxx
    key length              224

    key party               0
}
Log Format::=SEQUENCE{
    log serial number       xxxxxxxx
    purchace date           yyyy:mm:dd
    purchace time           hh:mm:ss
    content ID              xxxxxxxxxx
    purchace condition      xxx
    purchace limitation     xxxxxx
    purchace price          xxxxxx
    copy permission         xx
}
    ... ... ... ... ... ...
```

【００７１】上記で示したＲＭＰ仕様記述フォーマット

では、ＲＭＰの方式を識別するための識別情報（RMP ＩD）を冒頭に含む他、配信コンテンツを暗号化する暗号化アルゴリズム、配信コンテンツの暗号化に使用するコンテンツ・キーＫsを暗号化する暗号化アルゴリズム、コンテンツ配信時に使用する配信キーＫdを暗号化する暗号化アルゴリズム、配信コンテンツを蓄積するときに使用するストレージ・キーKst、相互認証に用いる認証アルゴリズム、ログを蓄積するためのフォーマットなどを規定することができる。暗号化方式としては、一般に、ＤＥＳ（Data Encription Standard）やＭｕｌｔｉ２などが使用される。

【００７２】ＲＭＰとしての仕様記述は、各コンテンツ制作・提供事業者毎に策定される。従来は、各コンテンツ配信システム毎にＲＭＰを固定して利用していたので、複数のシステムからコンテンツの提供を受けるためには、新しいコンテンツ受信機を用意するなど余計な出費が必要であった。これに対し、本発明では、ＲＭＰの仕様記述、並びにＲＭＰに入力するためのインターフェースを規定することにより、その仕様を解読するか、又はその仕様に適合したＲＭＰモジュールを入手することにより、同一のコンテンツ受信機上で、複数のコンテンツ配信システムにおけるコンテンツ課金、暗号化などのセキュリティ方式、著作権保護方式に対応することができる。

【００７３】本発明の１つの実現形態としては、コンテンツ受信機あるいはコンテンツ記録再生機内で、異なるＲＭＰ仕様を実装した複数のハードウェアＲＭＰモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアＲＭＰモジュールに切り替えて利用することが挙げられる。

【００７４】また、他の実現形態として、ソフトウェア・モジュールとしてＲＭＰモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードすることや、あるいは権利処理メタデータを解析して、所望のソフトウェア・モジュールをコンテンツ受信機側で自動生成することが挙げられる。

【００７５】図２には、異なるＲＭＰ仕様を実装した複数のハードウェアＲＭＰモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアＲＭＰモジュールに切り替えて利用する形式のコンテンツ受信機１０の構成を模式的に図解している。

【００７６】同図に示すコンテンツ受信機１０は、フロント・エンド部１１と、ＣＡＳ処理部１２と、コンテンツ蓄積用のハード・ディスク装置１３Ａ並びに１３Ｂと、ＲＭＰ識別部１４と、それぞれ異なるＲＭＰ仕様記述に基づく２つ（複数）のＲＭＰモジュール１並びにＲＭＰモジュール２とで構成される。

【００７７】フロント・エンド部１１は、所定チャネルの放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。

【００７８】ＣＡＳ処理部１２は、コンテンツ配信事業者との間で交わされたＣＡＳ（Conditional Access System（限定受信））に関する契約に基づき、放送コンテンツに適用されたスクランブル処理の解除（デスクランブル）を行う。日本国内のデジタル放送では、ＢＳ、ＣＳともに共通の"ＭＵＬＴＩ２"と呼ばれるスクランブル方式を採用する。但し、ＣＡＳ処理自体は本発明の要旨に関連しないので、ここではこれ以上説明しない。

【００７９】ハード・ディスク装置１３Ａ及び１３Ｂは、受信コンテンツの蓄積に使用される。より具体的には、一方のハード・ディスク装置１３ＡはＲＭＰモジュールによる権利処理前の状態のコンテンツの蓄積に使用され、他方のハード・ディスク装置１３Ｂは権利処理後の状態のコンテンツの蓄積に使用される。但し、ハード・ディスク装置１３Ａ及び１３Ｂは、物理的に互いに独立した装置である必要はなく、例えば、単一のハード・ディスク上に割り当てられた別個の記憶領域（パーティション）であってもよい。

【００８０】本実施例では、権利処理メタデータの一部として記述されるＲＭＰには、その方式を識別するための固有の識別情報（ＲＭＰ　ＩＤ）が割り振られている。ＲＭＰ識別部１４は、ハード・ディスク装置１３Ａから権利処理メタデータを読み出して、ＲＭＰ　ＩＤを識別して、２つ（複数）のＲＭＰモジュール１並びにＲＭＰモジュール２のうち識別されたＲＭＰ　ＩＤに対応する方を動作可能にする。

【００８１】ＲＭＰモジュール１並びにＲＭＰモジュール２は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース（前述）を備えている。ＲＭＰ識別部１４により付勢されたＲＭＰモジュール１又はＲＭＰモジュール２は、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置１３Ｂやリムーバブル・メディアへの格納などのコンテンツ処理を行う。

【００８２】また、図３には、他の実施形態に係るコンテンツ受信機２０の構成を模式的に図解している。コンテンツ受信機２０は、異なるＲＭＰ仕様を実装した複数のハードウェアＲＭＰモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアＲＭＰモジュールに切り替えて利用するようになっている。

【００８３】同図に示す例では、コンテンツ受信機２０は、フロント・エンド部２１と、ハード・ディスク装置２３と、ＲＭＰ識別部２４と、各ＲＭＰモジュール１及びＲＭＰモジュール２と、デコーダ出力装置２５が、同一のデータ・バス２６を介して相互接続された構成となっている。

【００８４】フロント・エンド部２１は、所定チャネル

の放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。但し、図示しないが、放送波を介さない代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部２１は、ネットワーク・インターフェース・カードで実現することができる。

【００８５】ハード・ディスク装置２３は、ＲＭＰモジュールによる権利処理前の状態のコンテンツを蓄積したり、権利処理後の状態のコンテンツを蓄積するために使用される。

【００８６】権利処理メタデータとして記述されるＲＭＰには、その方式を識別するための固有の識別情報ＲＭＰ　ＩＤが割り振られている。ＲＭＰ識別部２４は、ハード・ディスク装置２３から権利処理メタデータを読み出して、ＲＭＰ　ＩＤを識別して、２つ（複数）のＲＭＰモジュール１並びにＲＭＰモジュール２のうち識別されたＲＭＰ　ＩＤに対応するものを動作可能にする。

【００８７】ＲＭＰモジュール１並びにＲＭＰモジュール２は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース（前述）を備えている。ＲＭＰ識別部２４により付勢されたＲＭＰモジュール１又はＲＭＰモジュール２は、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置２３やリムーバブル・メディアへの格納などのコンテンツ処理を行う。なお、ＣＡＳ方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うＣＡＳモジュールをＲＭＰモジュール上に搭載するようにしてもよい。

【００８８】デコーダ出力装置２５は、権利処理後の再生コンテンツのデコード処理並びに外部出力を行う。例えば、ＡＶコンテンツであれば、デコーダ出力装置２５は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、ＭＰＥＧ２などによる圧縮映像データを伸張処理して、元のビデオ信号を再生するとともに、圧縮音声データに関しては、ＰＣＭ（Pulse Code Modulation）デコードした後に付加音と合成して再生音声信号とする。

【００８９】また、図４には、他の実施形態に係るコンテンツ受信機３０の構成を模式的に図解している。コンテンツ受信機３０は、ソフトウェア・モジュールとしてＲＭＰモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードするようになっている。

【００９０】同図に示すように、コンテンツ受信機３０は、フロント・エンド部３１と、ＣＰＵ（Central Processing Unit）３２と、ハード・ディスク装置３３Ａ及び３３Ｂと、ＲＭＰ識別部３４と、作業メモリ３５と、デコーダ出力装置３６と、ネットワーク・インターフェース３７が、システム・バス３８を介して相互接続された構成となっている。

【００９１】フロント・エンド部３１は、所定チャネルの放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。

【００９２】ネットワーク・インターフェース３７は、ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）などの所定の通信プロトコルに従ってコンテンツ受信機３７をインターネットなどの広域ネットワークに接続するための装置である。インターネット上には無数のホスト端末が接続されている。ホスト端末の一部は、映画や音楽などのコンテンツを配信する情報配信サーバであり、他の一部はソフトウェアＲＭＰモジュールを配信するサーバである。なお、放送経由でコンテンツを受信する代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部３１は、ネットワーク・インターフェース３７によって実現することができる。

【００９３】ＣＰＵ３２は、オペレーティング・システム（ＯＳ）の制御下で、コンテンツ受信機３０内の動作を統括的に制御する中央コントローラであり、作業メモリ３５を用いて各種のプログラム・コードを実行する。

【００９４】ハード・ディスク装置３３Ａは、ＲＭＰモジュールによる権利処理前の状態でのコンテンツの蓄積、並びに、権利処理後の状態のコンテンツの蓄積に使用される。また、ハード・ディスク装置３３Ｂは、以前使用した（あるいはあらかじめダウンロードしておいた）ソフトウェアＲＭＰモジュールの蓄積に利用される。ハード・ディスク装置３３Ａと３３Ｂは、それぞれ独立した装置ユニットである必要はなく、例えば単一のハード・ディスク装置上で区切られた記憶領域（例えばパーティション）であってもよい。

【００９５】権利処理メタデータとして記述されるＲＭＰには、その方式を識別するための固有の識別情報ＲＭＰ　ＩＤが割り振られている。ＲＭＰ識別部３４は、ハード・ディスク装置３３から権利処理メタデータを読み出して、ＲＭＰ　ＩＤを識別して、該当するソフトウェアＲＭＰモジュールが作業メモリ３５上にロードされて現在使用中か否かを検出する。ＲＭＰ識別部３４は、ハードウェア・コンポーネントとしてではなく、ＣＰＵ３２が実行するプログラム・コードとして実装することもできる。

【００９６】作業メモリ３５上のソフトウェアＲＭＰモジュールが、これから再生するコンテンツに関するＲＭＰ　ＩＤにヒットしない場合には、該当するソフトウェアＲＭＰモジュールをローカル・ディスク３３Ｂ上で探索し、見つかった場合にはこれを作業メモリ３５上のも

のと置き換える。ローカル・ディスク３３Ｂ上で該当するソフトウェアＲＭＰモジュールを発見することができなかった場合には、さらに、ネットワーク・インターフェース３７経由でネットワーク上のサーバにアクセスして、所望のソフトウェアＲＭＰモジュールを探索することができる。

【００９７】ＣＰＵ３２は、作業メモリ３５上にロードされたソフトウェアＲＭＰモジュールを実行することにより、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置３３Ａやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができる。なお、ＣＡＳ方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うＣＡＳモジュールを同様に作業メモリ３５上にロードすればよい。

【００９８】デコーダ出力装置３６は、権利処理後の再生コンテンツのデコード処理並びに外部出力を行う。例えば、ＡＶコンテンツであれば、デコーダ出力装置３６は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、ＭＰＥＧ２などによる圧縮映像データを伸張処理して元のビデオ信号を再生するとともに、圧縮音声データに関してはＰＣＭ（Pulse Code Modulation）デコードした後に付加音と合成して再生音声信号とする。

【００９９】図５には、コンテンツ受信機３０にソフトウェアＲＭＰモジュールをダウンロードするための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、ソフトウェア・モジュールのダウンロード処理について説明する。

【０１００】ハード・ディスク装置３３Ａに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置３３Ａから読み出して、ＲＭＰモジュールのＲＭＰ　ＩＤを取得する（ステップＳ１）。そして、このＲＭＰ　ＩＤが現在作業メモリ３５にロードされているＲＭＰモジュールのそれと一致するか否かをチェックする（ステップＳ２）。

【０１０１】ＲＭＰ　ＩＤがヒットする、すなわち、これから再生するコンテンツのＲＭＰモジュールが既に作業メモリ３５上にロードされている場合には、続いて管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ３）、コンテンツ再生を行い（ステップＳ４）、本処理ルーチン全体を終了する。

【０１０２】他方、ＲＭＰ　ＩＤがヒットしなかった場合には、ＲＭＰ入手先情報を取得して（ステップＳ５）、ＲＭＰ入手先となるサーバに接続して（ステップＳ６）、該当するソフトウェアＲＭＰモジュールをこのサーバからダウンロードする（ステップＳ７）。そして、ダウンロードしたソフトウェアＲＭＰモジュールをコンテンツ受信機３０にインストール（例えば、作業メモリ３５上にロード）する（ステップＳ８）。

【０１０３】ＲＭＰ入手先情報は、例えば権利処理メタデータ内にＵＲＬ（Uniform Resource Locator）形式で記述されている。このような場合、コンテンツ受信機３０は、ネットワーク・インターフェース３７経由でインターネットのようなＴＣＰ／ＩＰネットワーク経由でＵＲＬで指示されたサーバに対し資源アクセスして、該当するＲＭＰモジュールをＨＴＴＰ（Hyper Text Transfer Protocol）又はＦＴＰ（File Transfer Protocol）などの転送プロトコルに従ってダウンロードすることができる。

【０１０４】新規のソフトウェアＲＭＰモジュールをインストールした結果、コンテンツ受信機３０上において、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置３３Ａやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【０１０５】続いて、管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ３）、コンテンツ再生を行い（ステップＳ４）、本処理ルーチン全体を終了する。

【０１０６】ソフトウェア・モジュールとしてＲＭＰモジュールを構成する変形例として、ＣＰＵ３２（あるいは他の演算処理ユニット）が権利処理メタデータ内のＲＭＰ仕様記述を解析して、所望のソフトウェアＲＭＰモジュールをコンテンツ受信機３０内部で自動生成するようにしてもよい。

【０１０７】図６には、ソフトウェアＲＭＰモジュールをコンテンツ受信機３０内部で自動生成するための処理手順をフローチャートの形式で図解している。以下、このフローチャートに従って、ソフトウェアＲＭＰモジュールの自動生成処理について説明する。

【０１０８】ハード・ディスク装置３３Ａに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置３３Ａから読み出して、ＲＭＰモジュールのＲＭＰ　ＩＤを取得する（ステップＳ１１）。そして、このＲＭＰ　ＩＤが現在作業メモリ３５にロードされているＲＭＰモジュールのそれと一致するか否かをチェックする（ステップＳ１２）。

【０１０９】ＲＭＰ　ＩＤがヒットする、すなわち、これから再生するコンテンツのＲＭＰモジュールが既に作業メモリ３５上にロードされている場合には、続いて管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ１３）、コンテンツ再生を行い（ステップＳ１４）、本処理ルーチン全体を終了する。

【０１１０】他方、ＲＭＰ　ＩＤがヒットしなかった場合には、ＲＭＰ仕様記述に関する情報を権利処理メタデータから取得する（ステップＳ１５）。次いで、コンテンツ受信機３０上のコンピューテーション・パワー（例えば、ＣＰＵ３２が持つ計算能力）がＲＭＰモジュールを生成するに足りるか否かをチェックする（ステップＳ１６）。

【０１１１】コンピューテーション・パワー不足の場合には、コンテンツの再生が不可である旨のメッセージを表示した後（ステップＳ１９）、本処理ルーチンを異常終了する。

【０１１２】他方、コンピューテーション・パワーが充分であった場合には、さらに、ＲＭＰ仕様記述を解読して（ステップＳ１７）、作業メモリ３５上でＲＭＰを設定する（ステップＳ１８）。新規にＲＭＰを設定した結果、コンテンツ受信機３０上において、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置３３Ａやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【０１１３】続いて、管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ１３）、コンテンツ再生を行い（ステップＳ１４）、本処理ルーチン全体を終了する。

【０１１４】なお、ハードウェア・モジュールとしてＲＭＰモジュールを構成した場合、ソフトウェアによりモジュールを実装する場合に比し、簡単に他のＲＭＰモジュールに置き換えることはできない。このような場合、サーバ側において、受信機に対応したＲＭＰに置き換えるような仕組みを提供してもよい。例えば、コンテンツ受信機側は、コンテンツのＩＤでサーバに問い合わせて、コンテンツの変換を依頼する。権利処理条件が整っていれば、所定のＲＭＰに変換することができ、変換後のコンテンツ（あるいは、あらかじめ同じコンテンツが用意されていることでもよい）を依頼元のコンテンツ受信機にダウンロードすることで、希望するコンテンツの復号化・再生を実現することができる。

【０１１５】次いで、コンテンツ・プロバイダが衛星放送を利用してコンテンツ配信を行うコンテンツ配信システムに対して本発明を適用した場合の実施例について説明する。

【０１１６】図７には、コンテンツ配信システム１００の概略的構成を図解している。同図に示すコンテンツ配信システム１００は、コンテンツを制作・提供する番組制作会社又は委託放送事業者からなるコンテンツ・プロバイダ２００と、制作・提供されたコンテンツを衛星放送波によって配信する衛星放送受託放送事業者（以下、単に「放送局」とする）３００と、各一般家庭などに設置されたコンテンツ配信対応衛星放送受信機（以下、単に「コンテンツ受信機」とする）４００とで構成される。コンテンツ受信機４００は、一般に、映像及び音声出力用のテレビジョン（ＴＶ）４５０と接続されている。

【０１１７】コンテンツ・プロバイダ２００と放送局３００との間では、コンテンツ制作・提供に関する委託契約が交わされており、コンテンツ・プロバイダ２００が制作（あるいは外部のコンテンツ・プロバイダから取得した）コンテンツは放送局３００に提供される。放送局３００は、コンテンツを暗号化して、これを衛星放送波にのせて各家庭内のコンテンツ受信機４００に向けて配信する。

【０１１８】コンテンツ・プロバイダ２００は、コンテンツ制作事業者としての番組制作会社２０１とは独立した、コンテンツ課金を管理する外部の管理センタ２０２のような決済専門の機関と契約していてもよい。このような場合、コンテンツ・プロバイダ２００はコンテンツを暗号化する鍵の管理を管理センタ２０２に委ね、管理センタ２０２はコンテンツ販売情報を渡す。

【０１１９】管理センタ２０１は、さらに外部の認証局２５０や他の決済機関と連動していてもよい。また、管理センタ２０２は、個々のコンテンツ受信機４００との間で定期的あるいは不定期的に接続され、コンテンツ受信機４００に対して暗号化コンテンツを利用可能にするための鍵情報を配布する。コンテンツ受信機４００は、配布された鍵情報を用い、ＲＭＰ仕様記述に基づいて、放送衛星３０１経由で受信した暗号化コンテンツを解読して利用に供する。また、コンテンツ受信機４００は、ハード・ディスク装置のような大容量外部記憶装置を内蔵しており、受信したコンテンツを蓄積することができる。

【０１２０】また、コンテンツ受信機４００から管理センタ２０１に対しては、コンテンツの再生ログなど課金情報が送られてくる。コンテンツ受信機４００側のユーザは、例えば、コンテンツ使用回数相当の課金額を管理センタに対して月々決済すればよい。決済方法は、現金納付、所定の金融機関への振り込み、プリペイド・カードによる予納、クレジット・カードによる信用決済、デビット・カードによる即時決済、電子マネーの利用などいずれでもよい。

【０１２１】図８には、コンテンツ制作並びに配信を行う放送局３００における構成を模式的に図解している。以下、図８を参照しながら、コンテンツ配信時における暗号化などの仕組みについて説明する。

【０１２２】コンテンツ暗号化部３１１は、コンテンツ・プロバイダから提供された映像や音楽などのコンテンツを、コンテンツ鍵（コンテンツ・キー）Ｋｃを用いて暗号化する。但し、コンテンツ・プロバイダから提供されるコンテンツは、コンテンツ・プロバイダにおいて策定されたＲＭＰ仕様記述に則った暗号化その他の権利処

理が適用されているものとする。

【０１２３】コンテンツ鍵暗号化部３１２は、配信鍵（ディストリビューション・キー）KDを用いてコンテンツ鍵Kcを暗号化する。

【０１２４】マルチプレクサ３１３は、コンテンツ暗号化部３１１から入力する暗号化コンテンツと、コンテンツ鍵暗号化部３１２から入力する暗号化コンテンツ鍵を多重化して、トランスポート・ストリームＴＳ（Transport Stream）を生成する。トランスポート・ストリームは、暗号化コンテンツにメタデータや、暗号化コンテンツ鍵が付加されたデータ・ストリームである。

【０１２５】ＣＡＳスクランブラ３１４は、コンテンツ受信機４００において限定受信させるべく、トランスポート・ストリームをスクランブルすなわち攪拌処理する。ＣＡＳにおける契約情報やスクランブル鍵などは、例えば図示しない暗号化装置により暗号化され、放送波にのせてコンテンツ受信機４００側に送信することができる。

【０１２６】図９には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例４００Ａの構成を模式的に示している。同図に示すコンテンツ受信機４００Ａは、受信したコンテンツをハード・ディスクなどの所定のローカル記憶装置に一旦蓄積した後でコンテンツの購入を決定するタイプである。以下、同図を参照しながらコンテンツ受信機４００Ａについて説明する。

【０１２７】ＣＡＳデスクランブラ４１１は、図示しないフロント・エンドにより受信されたデータを、放送局３００側から取得したスクランブル鍵を用いてデスクランブルして、トランスポート・ストリームを再現する。

【０１２８】デマルチプレクサ４１２は、トランスポート・ストリームを、暗号化コンテンツと暗号化コンテンツ鍵とに分離する。分離後、これらは権利処理前の状態のままハード・ディスク装置４１３Ａに一旦蓄積される。

【０１２９】ＲＭＰモジュール４２０は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置４１３Ａに蓄積したコンテンツを購入する際、まず、対応する権利処理メタデータが読み出され、その中からＲＭＰ識別情報（RMP ID）が検出され、適当なＲＭＰモジュールが選択的に動作しているものとする。

【０１３０】ＲＭＰモジュール４２０は、コンテンツ購入に関する契約を交わした（あるいはユーザ・アカウントを取得している）管理センタ２０２と接続して、コンテンツの配信鍵KDを購入する。コンテンツ鍵復号化部４２１は、権利処理メタデータから暗号化コンテンツ鍵を取り出して、これを配信鍵KDで復号化してコンテンツ鍵Kcを得る。後続のコンテンツ鍵再暗号化部４２２は、ＲＭＰモジュール４２０で規定されているコンテンツ蓄積用の鍵（ストレージ・キー）Ksを用いてコンテンツ鍵Kcを再暗号化する。

【０１３１】購入した暗号化コンテンツを、再暗号化されたコンテンツ鍵とともに、ハード・ディスク装置４１３Ａからハード・ディスク装置４１３Ｂに移動する。但し、ハード・ディスク装置４１３Ａと４１３Ｂは、物理的に独立した装置ユニットである必要はなく、同一のハード・ディスク内で権利処理前（購入前）と権利処理後（購入後）とで記憶領域（例えば、パーティション）を区切られたものであってもよい。

【０１３２】ＲＭＰモジュール４２０は、購入コンテンツのための配信鍵KDの購入や、購入コンテンツの移動などの処理ログを、課金データとして蓄積しておく。そして、定期的あるいは不定期的に管理センタ２０２に接続して、課金データを転送する。

【０１３３】また、図１０には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｂの構成を模式的に示している。同図に示すコンテンツ受信機４００Ｂは、受信したコンテンツを一旦ハード・ディスクなどのローカル記憶装置に蓄積した後、コンテンツを再生を行うタイプである。コンテンツ受信機４００Ｂは、上述したコンテンツ受信機４００Ａにより購入・蓄積された暗号化コンテンツの再生装置としても機能する。以下、同図を参照しながらコンテンツ受信機４００Ｂについて説明する。

【０１３４】ハード・ディスク装置４３３内には、ＲＭＰモジュール４４０で規定されたコンテンツ鍵Kcを用いて暗号化されたコンテンツと、ＲＭＰモジュール４４０で規定されているコンテンツ蓄積用の鍵（ストレージ・キー）Ksで暗号化された暗号化コンテンツ鍵が格納されている。

【０１３５】コンテンツ購入時には、コンテンツ鍵復号化部４４１は、ハード・ディスク装置４３３から該当する暗号化コンテンツ鍵を読み出して、これを規定された格納鍵Ksを用いて復号化して、コンテンツ鍵Kcを得る。

【０１３６】コンテンツ復号化部４４２は、購入したい暗号化コンテンツをハード・ディスク装置４３３から読み出して、これを復号化されたコンテンツ鍵Kcを用いて復号化し、元の映像又は音楽などのコンテンツを再現する。

【０１３７】ＡＰＳ処理部４４３は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやＣＧＭＳ－Ａなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【０１３８】図９及び図１０に示すようなコンテンツ受信機４００Ａによれば、コンテンツ・プロバイダは、ＣＡＳとは独立した暗号化システムによりコンテンツを配信することができる。すなわち、ＣＡＳに依存しないコ

ンテンツ配信システムなので、異なるＣＡＳ（異なる放送事業者）にまたがった共通のプラットフォーム上でコンテンツ購入に対する課金処理を行うことができる。この場合、ＣＡＳは、単なるコンテンツの流通経路に過ぎない。コンテンツは暗号化されたままの状態でハード・ディスク装置のようなローカル記憶装置に蓄積される。購入時に、コンテンツを解くための鍵がコンテンツ鍵Ｋcから格納鍵Ｋsにかけ変えられるので、その後は同じコンテンツ受信機４００Ａ上でいつでも再生することができる。また、コンテンツ購入処理時に課金するためのログが作成され、定期的あるいは不定期的に管理センタ２０２に送信されるので、コンテンツ利用者に対して確実に課金・決済を行うことができる。

【０１３９】図１１には、図９に示したようなコンテンツ受信機４００Ａにおいて、受信コンテンツをハード・ディスク装置４１３Ａに蓄積するための処理手順の一例をフローチャートの形式で示している。受信コンテンツは、基本的には、権利処理前のまま蓄積される。以下、このフローチャートに従って、コンテンツの蓄積処理について説明する。

【０１４０】まず、コンテンツ受信機４００Ａのユーザにより予約したい番組が決まっているか否か（すなわち予約設定されているか否か）をチェックする（ステップＳ２１）。

【０１４１】予約したい番組が既に決められている場合には、例えばデジタル放送であればデータ放送用データの中からＥＰＧ（Electric Program Guide：電子番組表）を取り出し、ＥＰＧを基に予約すべき番組を選択する（ステップＳ２２）。そして、予約すべき時刻（放映時間帯）並びにチャンネルなどを設定する（ステップＳ２３）。

【０１４２】次いで、ユーザからのプリファレンス入力（ステップＳ２４）を基に、プリファレンスにあった番組を所定の検索エンジンが自動選択する（ステップＳ２５）。そして、予約すべき時刻（時間帯）並びにチャンネルなどを設定する（ステップＳ２６）。

【０１４３】予約開始時刻に到達した、あるいは選択された番組ＩＤが受信されたことに応答して、ハード・ディスク装置への受信コンテンツの自動蓄積を行う（ステップＳ２７）。

【０１４４】また、図１２には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｃの構成を模式的に示している。同図に示すコンテンツ受信機４００Ｃは、ＩＣカード化された衛星放送用のＣＡＳモジュール、すなわちＢＳ－ＣＡＳ　ＩＣカードを内蔵しており、受信したコンテンツを一旦ハード・ディスク装置に蓄積した後、ＣＡＳシステムに基づいて衛星放送を限定受信して視聴するタイプである。以下、同図を参照しながら、コンテンツ受信機４００Ｃについて説明する。

【０１４５】図示しないフロント・エンドにより受信されたデータ・コンテンツは、権利処理前で且つＣＡＳによりスクランブル処理された状態のまま、ハード・ディスク装置４５３のような大容量記憶装置に一時蓄積される。

【０１４６】受信コンテンツの権利処理はＲＭＰモジュール４６０により行われる。ＲＭＰモジュール４６０は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置４５３に蓄積したコンテンツを購入する際、対応する権利処理メタデータが読み出され、ＲＭＰ識別情報（RMP ID）が検出され、適当なＲＭＰモジュールが選択的に動作しているものとする。図示の例では、ＩＣカードとして提供されるＣＡＳモジュールはＲＭＰモジュール４６０の一部を構成する。

【０１４７】蓄積されたコンテンツを再生する際、該当する権利処理メタデータをハード・ディスク装置４５３から読み出す。

【０１４８】権利処理メタデータ中には、ＥＣＭ（Entitlement Control Message）とＥＭＭ（Entitlement Management Message）が含まれている。ＥＣＭは、ＣＡＳスクランブルを解除するためのスクランブル鍵Ｋscを暗号化したものである。また、ＥＭＭは、ＥＣＭを解くためのワーク鍵を、契約期間などの契約内容やメッセージとともに暗号化したものである。

【０１４９】復号部４６２は、ＢＳ－ＣＡＳ　ＩＣカードに記録されているマスター鍵Ｋmを用いてＥＭＭを解読してワーク鍵と契約情報を得る。次いで、復号部４６１は、ワーク鍵を用いてＥＣＭを解読して、スクランブル鍵Ｋscを得る。

【０１５０】判定部４６４は、復号部４６２において得られた契約情報に基づき、コンテンツ受信機４００Ｃの正当性を検証する。正当と判定した場合、スクランブル鍵Ｋscを復号部４６５に供給する。

【０１５１】ハード・ディスク装置４５３に蓄積された受信コンテンツは、ＣＡＳに基づき、Ｍｕｌｔｉ２などの方式によりスクランブル処理されている。復号部４６５は、再生すなわち視聴したいコンテンツをハード・ディスク装置４５３から取り出して、スクランブル鍵Ｋscを用いてデスクランブル処理する。

【０１５２】ＡＰＳ処理部４６６は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやＣＧＭＳ－Ａなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【０１５３】一方、復号部４６２において得られた契約情報は、ＰＰＶデータ格納部４６３に蓄積される。ＲＭＰモジュール４６０は、定期的あるいは不定期的に管理センタ２０２に接続して、ＰＰＶデータを転送する。管理センタ２０２は、ＰＰＶデータを基に、コンテンツ利

用者に対する課金処理を行うことができる。

【０１５４】図１２に示すコンテンツ受信機４００Ｄの構成によれば、ＣＡＳをそのまま蓄積コンテンツの課金に利用することができる。ＣＡＳに従って暗号化されたコンテンツは、暗号化されたままハード・ディスク装置に蓄積される。ＣＡＳで使用されるマスター鍵Ｋｍによりｅｍｍ並びにｅｃｍを解いて、蓄積コンテンツを解くことができる。その際、暗号を解いたことを課金ログとして記録する。このような課金ログを定期的あるいは不定期的に管理センタに送信することで、コンテンツ利用者に対して確実に課金を行うことができる。

【０１５５】また、図１３には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｄの構成を模式的に示している。同図に示すコンテンツ受信機４００Ｄは、ＩＣカード化された衛星放送用のＣＡＳモジュール、すなわちＢＳ－ＣＡＳ　ＩＣカードを内蔵しており、ＣＡＳシステムに基づいて衛星放送を限定受信してＣＡＳデスクランブルを行った後、再度暗号化してハード・ディスク装置に蓄積するタイプである。以下、同図を参照しながら、コンテンツ受信機４００Ｄについて説明する。

【０１５６】受信コンテンツの権利処理はＲＭＰモジュール４８０により行われる。ＲＭＰモジュール４８０は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。フロント・エンド部（図示しない）よりコンテンツが受信されたときに、対応する権利処理メタデータが読み出され、ＲＭＰ識別情報（ＲＭＰ ＩＤ）が検出され、適当なＲＭＰモジュールが選択的に動作しているものとする。同図に示す例では、ＩＣカードとして提供されるＣＡＳモジュールや、ハード・ディスク装置に蓄積するコンテンツの保護を行うセキュア・モジュールは、ＲＭＰモジュール４８０の一部を構成する。セキュア・モジュールは、ハード・ディスク装置に蓄積するコンテンツの再暗号化処理、並びに、再生時の暗号解除処理を行う。

【０１５７】図示しないフロント・エンドにより受信されたデータ・コンテンツのうち、権利処理メタデータは、ＣＡＳモジュールすなわちＢＳ－ＣＡＳ　ＩＣカードに入力される。

【０１５８】権利処理メタデータ中には、ＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ）とＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ）が含まれている。復号部４８２は、ＢＳ－ＣＡＳ　ＩＣカードに記録されているマスター鍵Ｋｍを用いてＥＭＭを解読してワーク鍵と契約情報を得る。次いで、復号部４８１は、ワーク鍵を用いてＥＣＭを解読して、スクランブル鍵Ｋｓｃを得る。また、復号部４８２において得られた契約情報は、ＰＰＶデータ格納部４８３に蓄積される。

【０１５９】判定部４８４は、復号部４８２において得られた契約情報に基づき、コンテンツ受信機４００Ｄの正当性を検証する。正当と判定した場合、スクランブル鍵Ｋｓｃを復号部４８５に供給する。

【０１６０】復号部４８５は、スクランブル鍵Ｋｓｃを用いて受信コンテンツをデスクランブル処理して、セキュア・モジュールに出力する。

【０１６１】セキュア・モジュール内では、暗号化部４８７が、コンテンツ受信機４００Ｄに固有のコンテンツ蓄積鍵Ｋｓｔを用いてＣＡＳデスクランブル後のコンテンツを再度暗号化して、ハード・ディスク装置４７３に格納する。

【０１６２】また、ハード・ディスク装置４７３に蓄積しておいたコンテンツを再生すなわち視聴する場合には、暗号化コンテンツをハード・ディスク装置４７３から読み出し、復号部４８８にてコンテンツ蓄積鍵Ｋｓｔを用いて復号化する。そして、ＡＰＳ処理部４８９は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやＣＧＭＳ－Ａなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【０１６３】また、セキュア・モジュール内では、ＣＡＳデスクランブル処理後のコンテンツから権利処理メタデータが取り出され、課金データとして蓄積される。

【０１６４】ＲＭＰモジュール４８０は、定期的あるいは不定期的に管理センタ２０２に接続して、ＣＡＳモジュールにて蓄積されたＰＰＶデータや、セキュア・モジュールにて蓄積された課金データを転送する。管理センタ２０２は、ＰＰＶデータを基に、コンテンツ利用者に対する課金処理を行うことができる。

【０１６５】図１３に示すような構成のコンテンツ受信機４００Ｄによれば、ＣＡＳシステムに従って配信されるコンテンツを再度暗号化して、ハード・ディスク装置に蓄積することができる。再暗号化の際、ＣＡＳで使用するスクランブル鍵Ｋｓｃとは異なる鍵構造のコンテンツ蓄積鍵Ｋｓｔで暗号化する。ハード・ディスク装置に蓄積された暗号化コンテンツを再生する場合には、再生する度に課金ログを生成して、定期的あるいは不定期的に管理センタ２０２に送信して、コンテンツ利用者に対する課金を行う。ＣＡＳをＲＭＰモジュールと一体化して構成することもできる。

【０１６６】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１６７】

【発明の効果】以上詳記したように、本発明によれば、映画や音楽などの暗号化された形式で配信される有料コ

ンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【０１６８】また、本発明によれば、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【０１６９】また、本発明によれば、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【０１７０】また、本発明によれば、各コンテンツ配信システム毎に策定される複数のＲＭＰ（Right Management &; Protection）方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【０１７１】本発明に係るコンテンツ受信装置及びコンテンツ受信方法によれば、１台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができ、配信システム毎の受信機などの機器を用意する必要がなくなる。また、各コンテンツ制作・提供・配信事業者間では、ＲＭＰ仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性や融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【図面の簡単な説明】

【図１】ＲＭＰモジュールの概念構成を示した図である。

【図２】異なるＲＭＰ仕様を実装した複数のハードウェアＲＭＰモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアＲＭＰモジュールに切り替えて利用する形式のコンテンツ受信機の構成を模式的に示した図である。

【図３】異なるＲＭＰ仕様を実装した複数のハードウェアＲＭＰモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアＲＭＰモジュールに切り替えて利用する形式のコンテンツ受信機２０の他の構成例を模式的に示した図である。

【図４】ソフトウェア・モジュールとしてＲＭＰモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードする形式のコンテンツ受信機３０の他の構成例を模式的に示した図である。

【図５】コンテンツ受信機３０にＲＭＰモジュールをダウンロードするための処理手順を示したフローチャートである。

【図６】ソフトウェアＲＭＰモジュールをコンテンツ受信機３０内部で自動生成するための処理手順を示したフローチャートである。

【図７】コンテンツ配信システムの概略的構成を示した図である。

【図８】コンテンツ制作並びに配信を行う放送局における構成を模式的に示した図である。

【図９】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例４００Ａの構成を模式的に示した図である。

【図１０】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｂの構成を模式的に示した図である。

【図１１】図９に示したコンテンツ受信機４００Ａにおいて、受信コンテンツをハード・ディスク装置４１３Ａに蓄積するための処理手順の一例を示したフローチャートである。

【図１２】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｃの構成を模式的に示した図である。

【図１３】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｃの構成を模式的に示した図である。

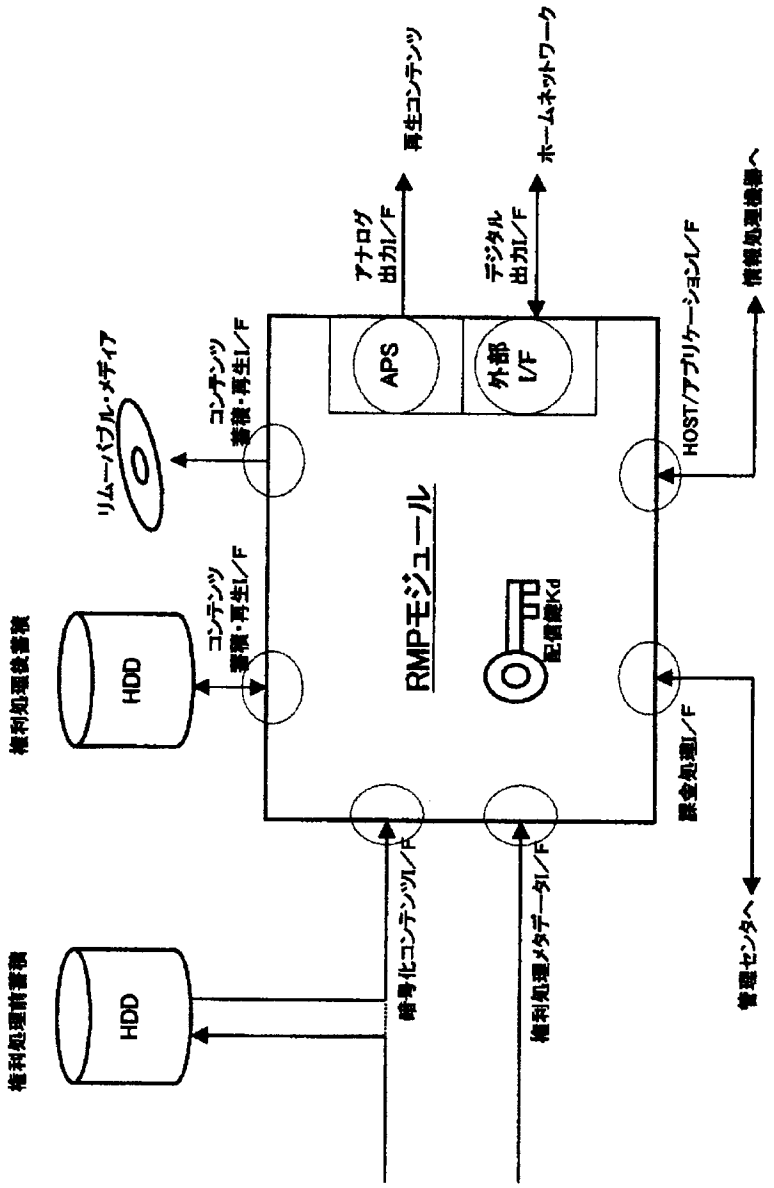
【図１４】ＣＡＳベースのコンテンツ配信システムの概観構成を示した図である。

【符号の説明】

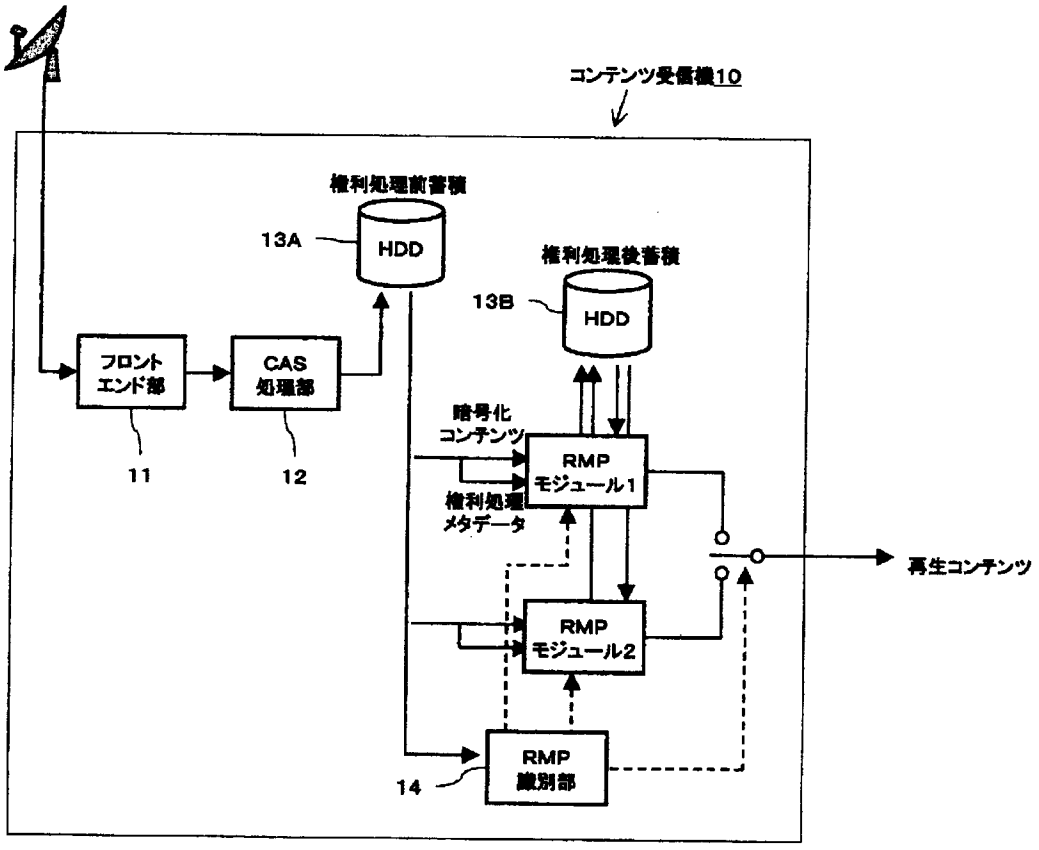
１０…コンテンツ受信機、１１…フロント・エンド部
１２…ＣＡＳ処理部、１３Ａ，１３Ｂ…ハード・ディスク装置
１４…ＲＭＰ識別部
２０…コンテンツ受信機、２１…フロント・エンド部
２３…ハード・ディスク装置、２４…ＲＭＰ識別部
２５…デコーダ出力装置
３０…コンテンツ受信機、３１…フロント・エンド部
３２…ＣＰＵ、３３Ａ，３３Ｂ…ハード・ディスク装置
３４…ＲＭＰ識別部、３５…作業メモリ
３６…デコーダ出力装置、３７…ネットワーク・インターフェース
２００…コンテンツ・プロバイダ
２０１…番組制作会社（委託放送事業者）、２０２…管理センタ（決済機関）
２５０…認証局
３００…放送局（衛星放送受託放送事業者）、３０１…放送衛星
３１１…コンテンツ暗号化部、３１２…コンテンツ鍵暗号化部
３１３…マルチプレクサ、３１４…ＣＡＳスクランブラ
４００…コンテンツ受信機（コンテンツ配信対応衛星放送受信機）

４１１…ＣＡＳデスクランブラ、４１２…デマルチプレクサ
４１３Ａ，４１３Ｂ…ハード・ディスク装置
４２０…ＲＭＰモジュール、４２１…コンテンツ鍵復号化部
４２２…コンテンツ鍵再暗号化部
４３３…ハード・ディスク装置、４４０…ＲＭＰモジュール
４４１…コンテンツ鍵復号化部、４４２…コンテンツ復号化部
４４３…ＡＰＳ処理部
４５３…ハード・ディスク装置、４６０…ＲＭＰモジュール
４６１…復号部、４６２…復号部
４６３…ＰＰＶデータ格納部、４６４…判定部
４６５…復号部、４６６…ＡＰＳ処理部
４７３…ハード・ディスク装置、４８０…ＲＭＰモジュール
４８１…復号部、４８２…復号部
４８３…ＰＰＶデータ格納部、４８４…判定部
４８５…復号部、４８７…暗号化部
４８８…復号部、４８９ＡＰＳ処理部

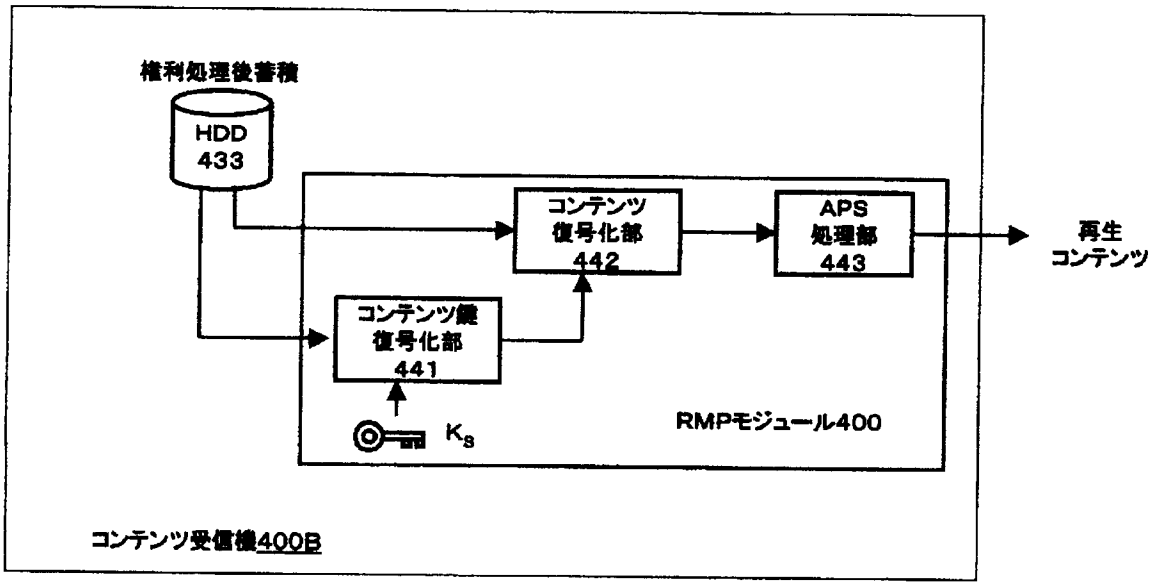
【図１】



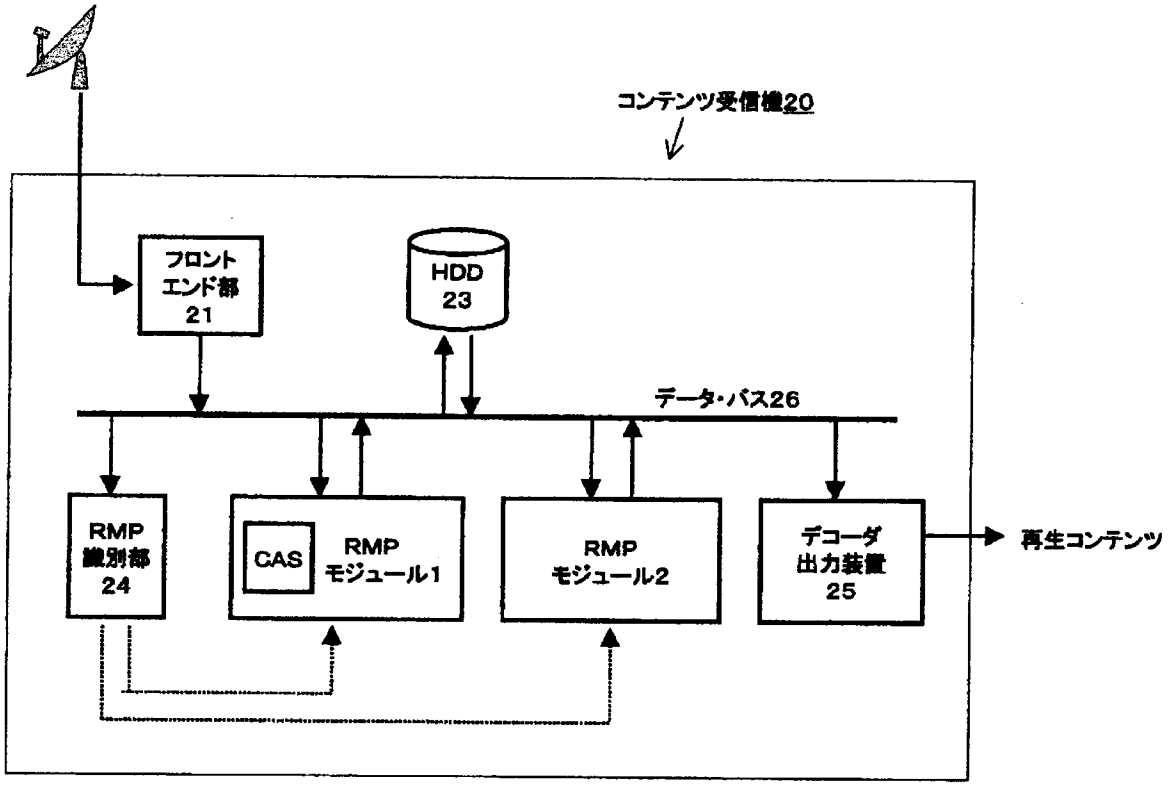
【図２】


コンテンツ受信機10
権利処理前蓄積
13A
HDD
権利処理後蓄積
13B
HDD
フロント
エンド部
CAS
処理部
11
12
暗号化
コンテンツ
RMP
モジュール1
権利処理
メタデータ
再生コンテンツ
RMP
モジュール2
RMP
識別部
14

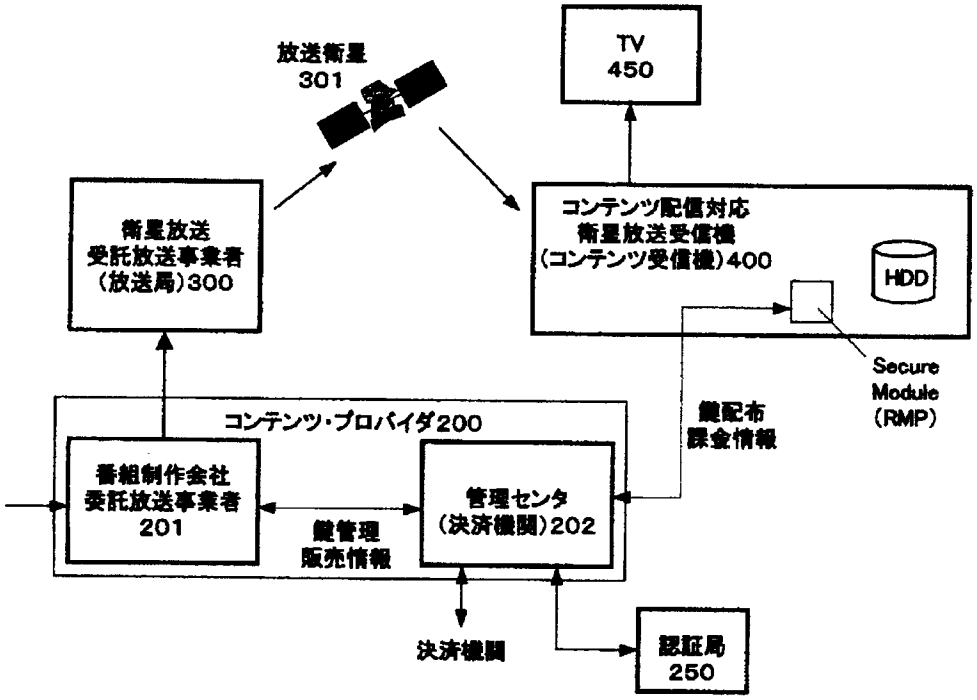
【図１０】


権利処理後蓄積
HDD
433
コンテンツ
復号化部
442
APS
処理部
443
再生
コンテンツ
コンテンツ鍵
復号化部
441
Ks
RMPモジュール400
コンテンツ受信機400B

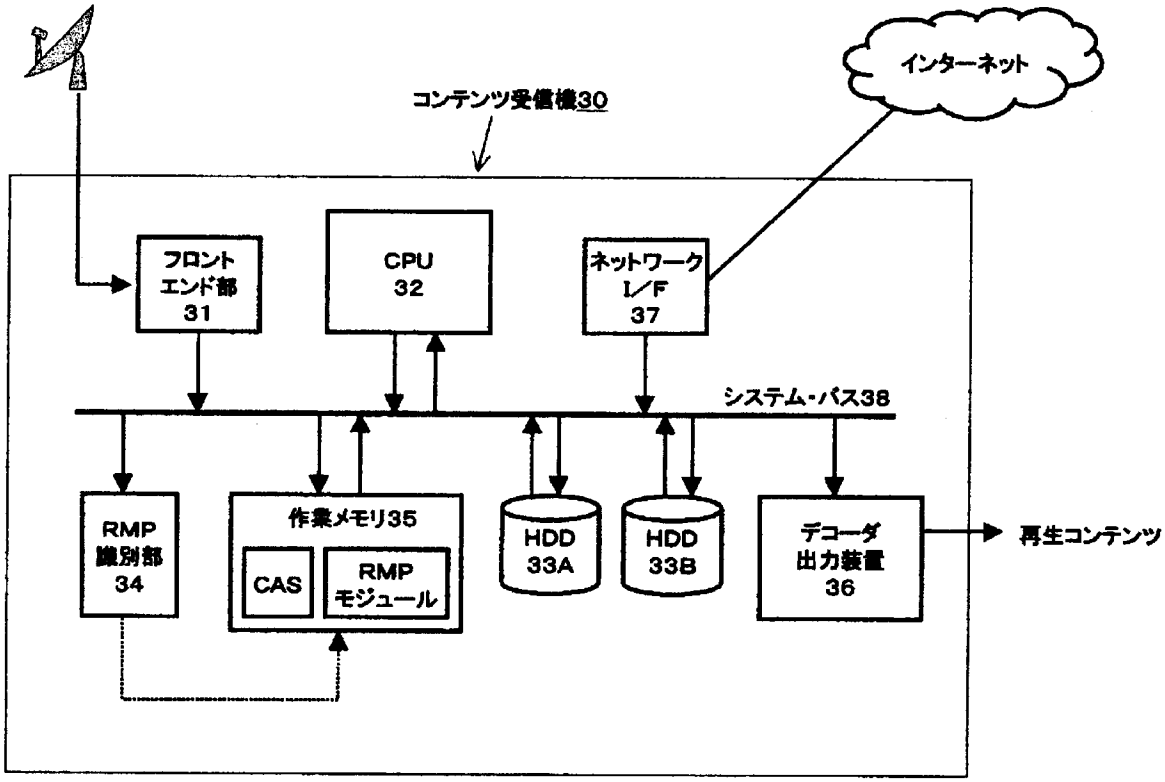
【図３】


コンテンツ受信機20
フロントエンド部21
HDD23
データ・バス26
RMP識別部24
CAS
RMPモジュール1
RMPモジュール2
デコーダ出力装置25
再生コンテンツ

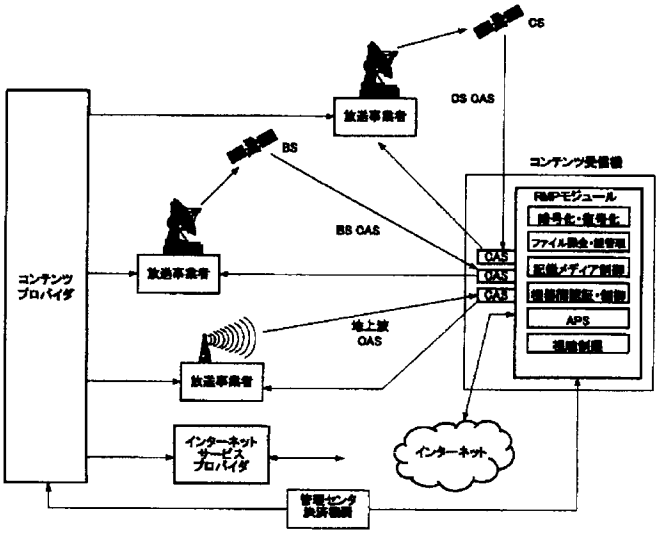
【図７】


放送衛星301
TV450
衛星放送受託放送事業者（放送局）300
コンテンツ配信対応衛星放送受信機（コンテンツ受信機）400
HDD
Secure Module (RMP)
コンテンツ・プロバイダ200
鍵配布課金情報
番組制作会社委託放送事業者201
管理センタ（決済機関）202
鍵管理販売情報
決済機関
認証局250

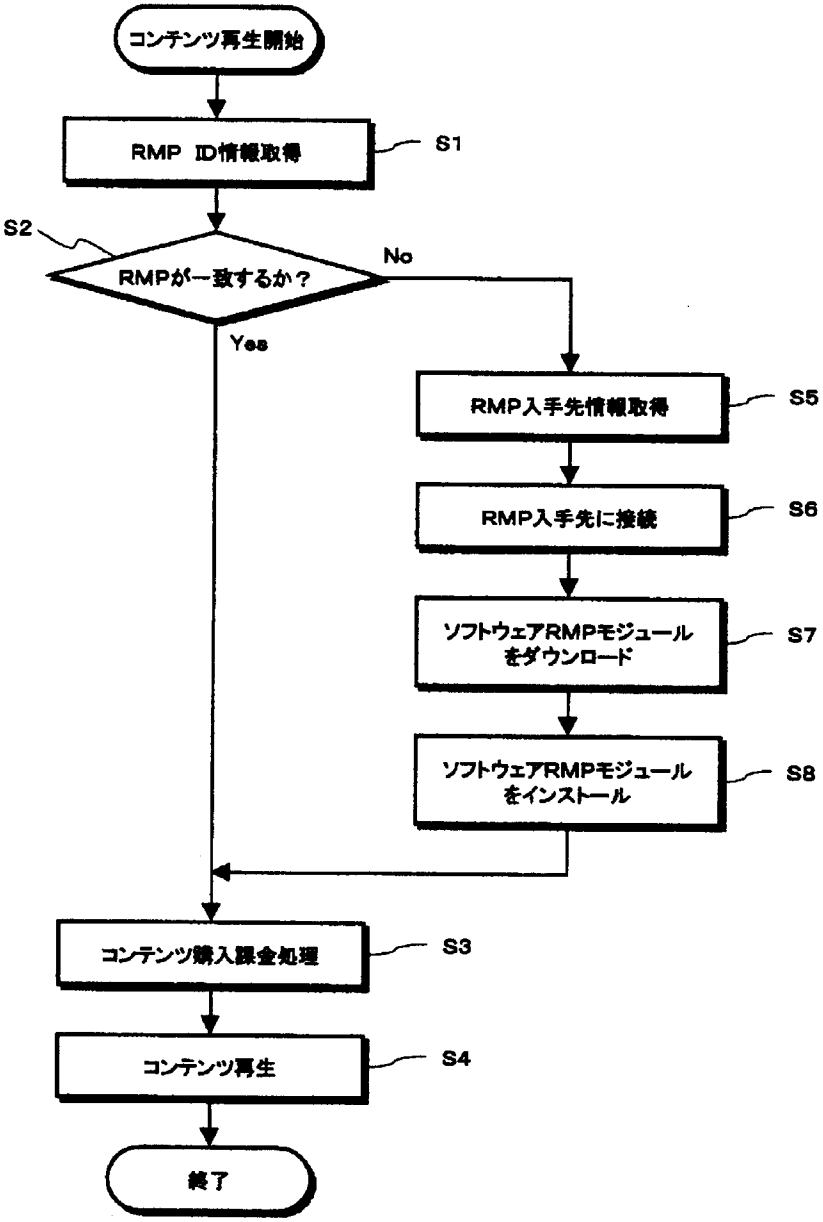
【図４】


インターネット
コンテンツ受信機30
フロント
エンド部
31
CPU
32
ネットワーク
I／F
37
システム・バス38
RMP
識別部
34
作業メモリ35
CAS
RMP
モジュール
HDD
33A
HDD
33B
デコーダ
出力装置
36
再生コンテンツ

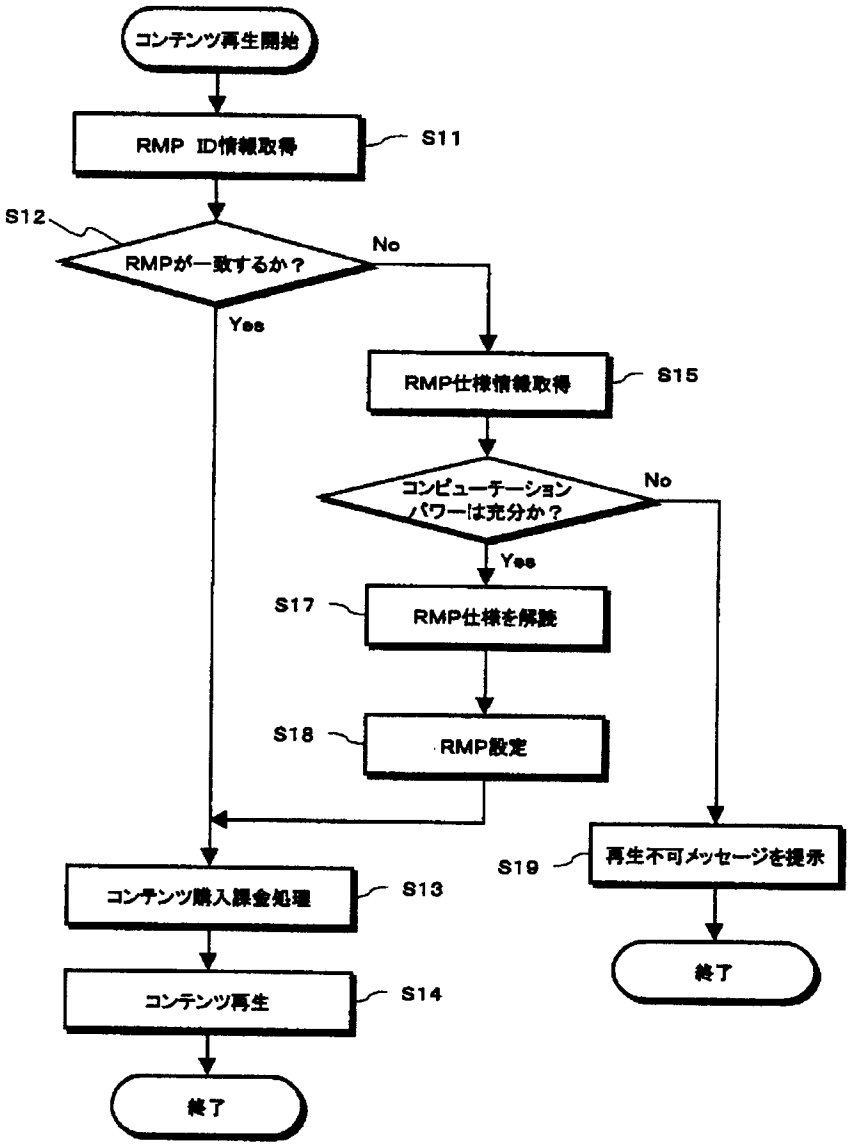
【図１４】


CS
CS CAS
放送事業者
BS
BS CAS
コンテンツ受信機
RMPモジュール
CAS
CAS
CAS
APS
コンテンツ
プロバイダ
放送事業者
地上波
CAS
放送事業者
インターネット
サービス
プロバイダ
インターネット

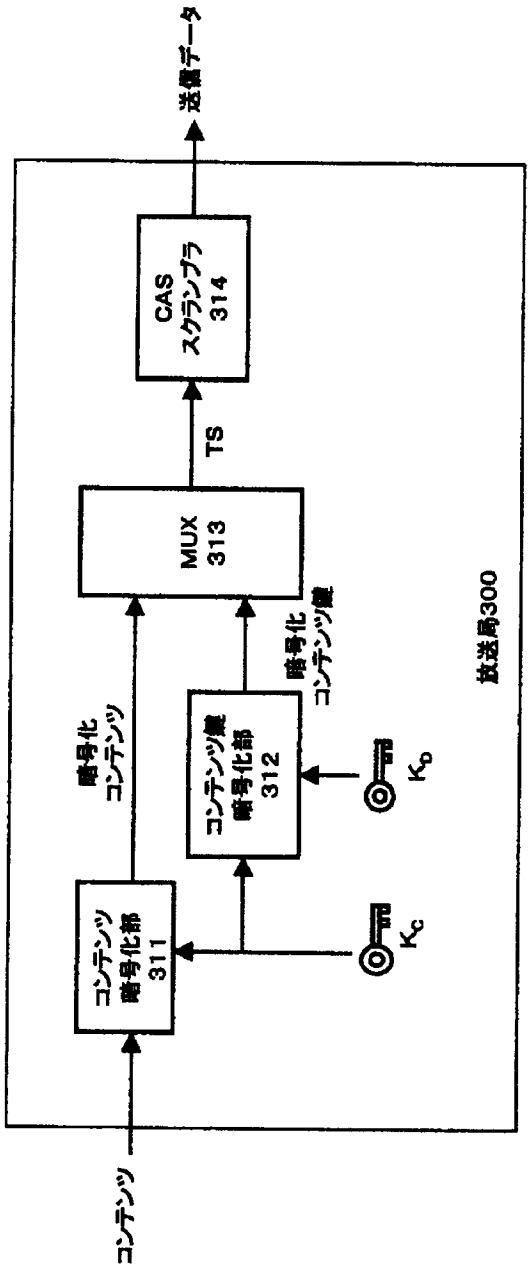
【図５】


コンテンツ再生開始
RMP ID情報取得
S1
S2
RMPが一致するか？
No
Yes
RMP入手先情報取得
S5
RMP入手先に接続
S6
ソフトウェアRMPモジュール
をダウンロード
S7
ソフトウェアRMPモジュール
をインストール
S8
コンテンツ購入課金処理
S3
コンテンツ再生
S4
終了

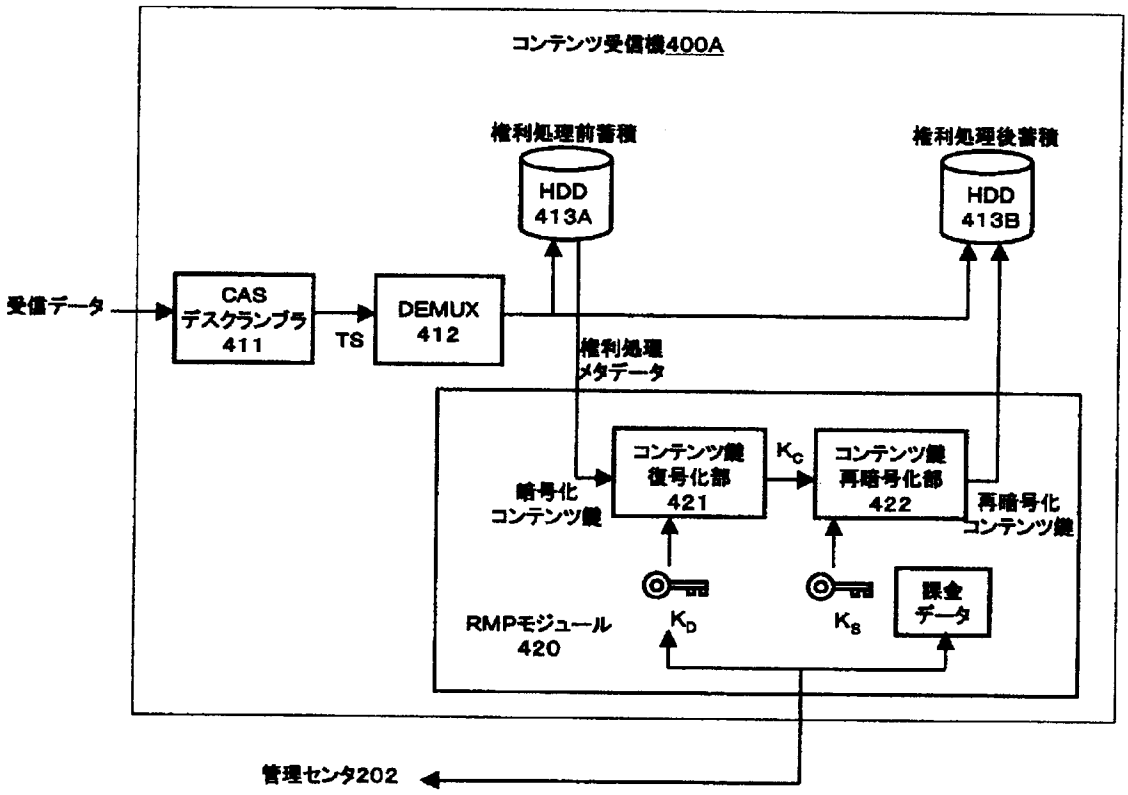
【図６】


コンテンツ再生開始
RMP ID情報取得
S11
S12
RMPが一致するか？
No
Yes
RMP仕様情報取得
S15
コンピューテーション
パワーは充分か？
No
Yes
S17
RMP仕様を解読
S18
RMP設定
S19
再生不可メッセージを提示
終了
コンテンツ購入課金処理
S13
コンテンツ再生
S14
終了

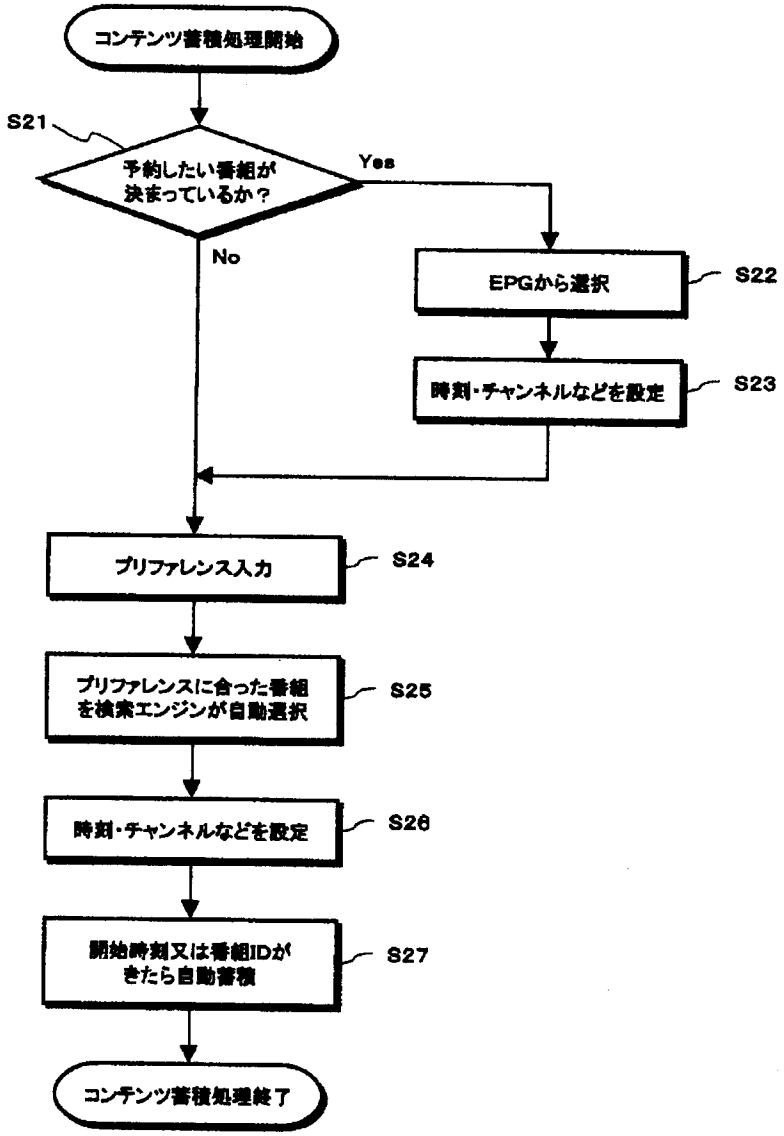
【図８】


送信データ
CAS
スクランブラ
314
TS
MUX
313
暗号化
コンテンツ鍵
暗号化
コンテンツ
コンテンツ鍵
暗号化部
312
コンテンツ
暗号化部
311
$K_D$
$K_C$
コンテンツ
放送局300

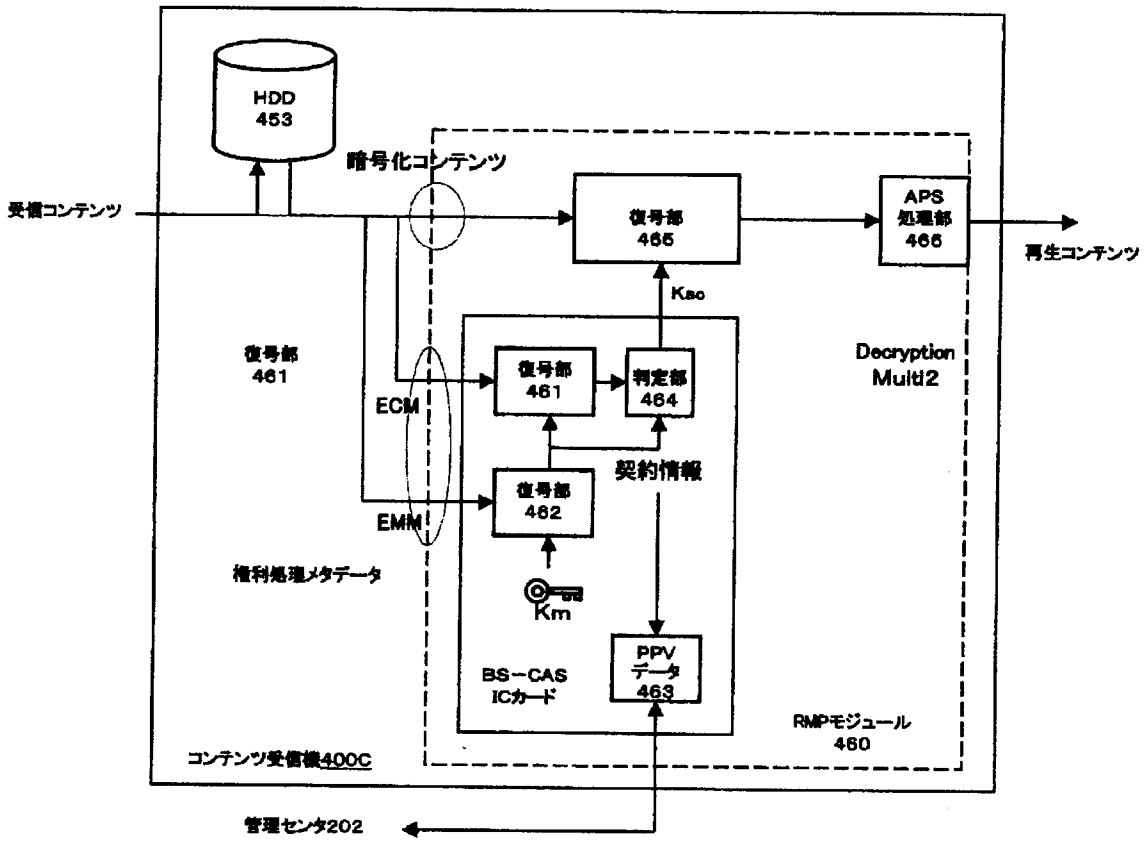
【図９】


コンテンツ受信機400A
権利処理前蓄積
HDD
413A
権利処理後蓄積
HDD
413B
受信データ
CAS
デスクランブラ
411
TS
DEMUX
412
権利処理
メタデータ
暗号化
コンテンツ鍵
コンテンツ鍵
復号化部
421
$K_C$
コンテンツ鍵
再暗号化部
422
再暗号化
コンテンツ鍵
RMPモジュール
420
$K_D$
$K_S$
課金
データ
管理センタ202

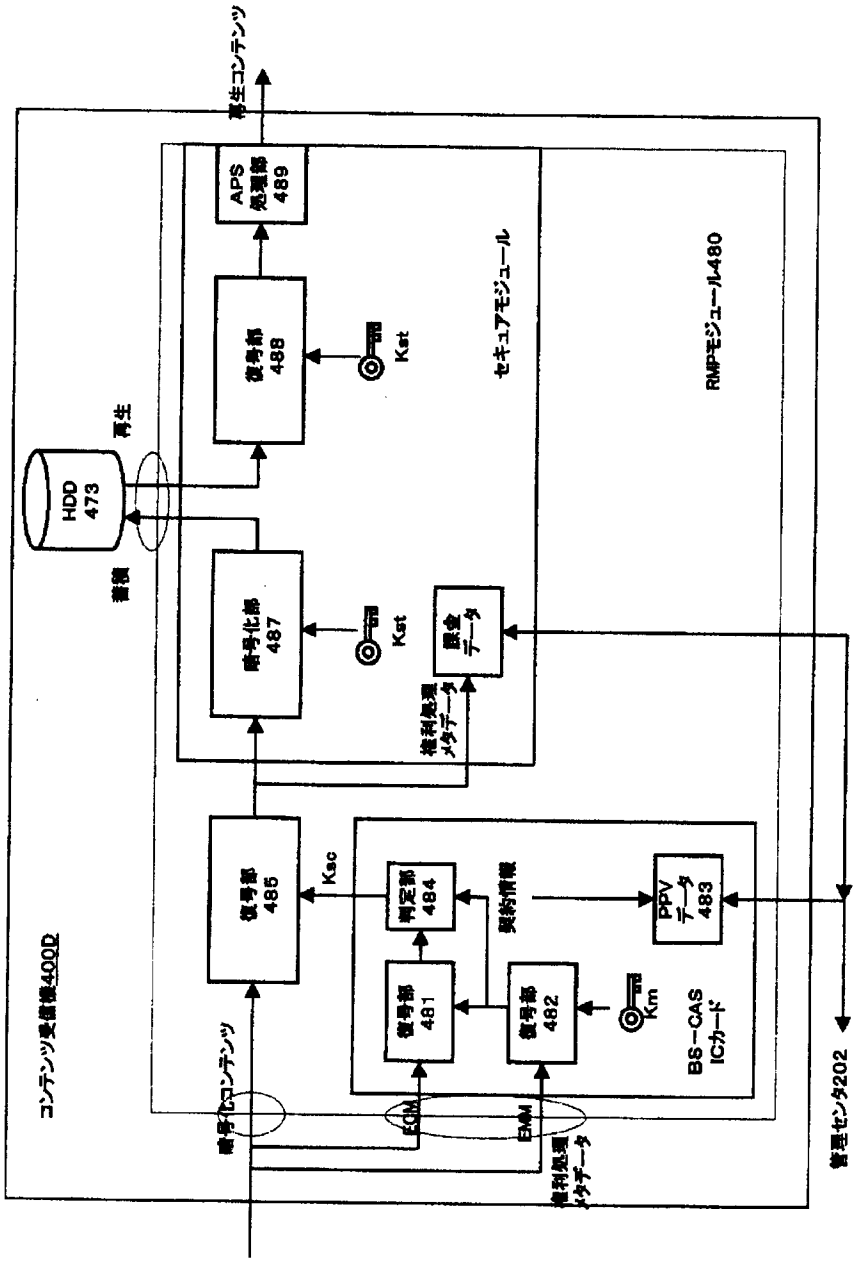
【図１１】


コンテンツ蓄積処理開始
S21
予約したい番組が決まっているか？
Yes
No
EPGから選択
S22
時刻・チャンネルなどを設定
S23
プリファレンス入力
S24
プリファレンスに合った番組を検索エンジンが自動選択
S25
時刻・チャンネルなどを設定
S26
開始時刻又は番組IDがきたら自動蓄積
S27
コンテンツ蓄積処理終了

【図１２】


HDD
453
暗号化コンテンツ
受信コンテンツ
復号部
465
APS
処理部
466
再生コンテンツ
Kso
復号部
461
Decryption
Multi2
復号部
461
判定部
464
ECM
契約情報
復号部
462
EMM
権利処理メタデータ
Km
PPV
データ
463
BS－CAS
ICカード
RMPモジュール
460
コンテンツ受信機400C
管理センタ202

【図１３】




フロントページの続き

| (51) Int. Cl.⁷ | 識別記号 | F I | | ﾃｰﾏｺｰﾄﾞ（参考） |
|---|---|---|---|---|
| H04N 7/167 | | H04L 9/00 | 601E | |
| | | H04N 7/167 | Z | |

Ｆターム(参考) 5B085 AA08 AE00 AE29
5C025 BA25 BA27 DA04 DA05
5C064 BA01 BB01 BC03 BC06 BC22
BC25 BD04 BD09 BD14 CA14
5J104 AA01 AA12 AA15 AA16 EA06
EA18 NA02 NA35 NA37 PA05
PA07 PA11